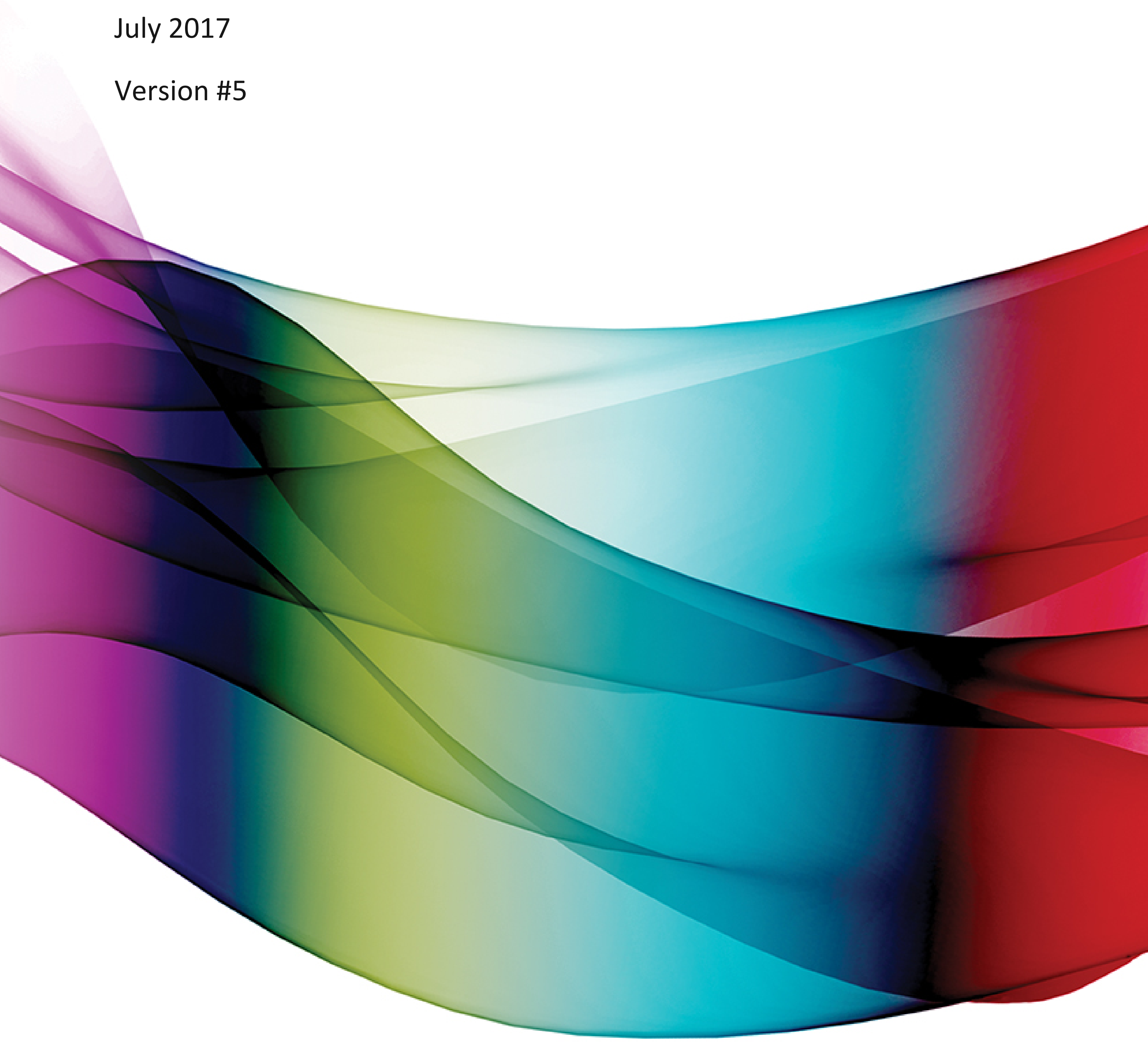
Acceptable Use of Technology Services Policy

July 2017

Version #5



Contents

1. Introduction and Purpose

TasNetworks seeks to provide its team members, contractors, consultants and visitors with secure and timely access TasNetworks' technology services, Infrastructure and Systems and the online services and resources necessary for undertaking their work.

TasNetworks is highly reliant on information that is gathered, stored, processed and delivered by technology Systems and their associated facilities.

The purpose of this Policy is to give a clear statement to all Users of TasNetworks' technology services, Infrastructure and Systems of their responsibilities, including:

- what constitutes acceptable and unacceptable use;
- the provision and modification of access to online services;
- code of conduct relating to use of social media;
- access to externally hosted TasNetworks Systems; and
- access to TasNetworks applications for external users.

2. Who does this Policy apply to?

This policy applies to all users of TasNetworks' technology services, Infrastructure and Systems, including:

- team members (employees, including full-time, part-time, contract, casual or fixed-term);
- contractors;
- consultants ; and
- contracted third parties (vendors) and their employees or contractors.

Hereafter known as "**Users**".

In some circumstances, visitors or customers of TasNetworks may be given access to TasNetworks' technology services, Infrastructure and Systems (other than external facing Systems such as the TasNetworks website) by a User. It is the User's responsibility to ensure that the visitor or customer who is given such access is made aware of this Policy and every reasonable effort is made to ensure that the visitor or customer complies with the requirements of this Policy during the course of their access.

This Policy sets out the context for fair and reasonable use of TasNetworks' technology services, Infrastructure and Systems and defines the various responsibilities of Users and TasNetworks' technology management teams to ensure that such usage is aligned with the TasNetworks Code of Conduct and does not cause risk to or hinder the operation of TasNetworks' business or its brand, legal or reputational standing in the community.

This Policy also includes the Social Media Code of Conduct and applies to all Users of TasNetworks' technology services, Infrastructure and Systems. The Social Media Code of Conduct applies to use of the following:

- Multi-media and social networking websites;
- External Blogs;
- External media websites (such as commenting on public news articles); and
- Wikis such as Wikipedia and any other site where text can be posted.

This Policy is applicable regardless of a User's location.

3. Policy Detail

3.1. Acceptable and Unacceptable Use of TasNetworks' Technology Services, Infrastructure and Systems

3.1.1 TasNetworks' technology services, Infrastructure and Systems are provided for use in the administrative, commercial and community activities of TasNetworks. Some reasonable and incidental, non-commercial personal use may be allowed, but as a privilege and not a right. If that privilege is abused it will be treated as a breach of this Policy. Refer to the TasNetworks Code of Conduct and the Alcohol and Other Drug Procedure.

3.1.2 Use of TasNetworks' technology services, Infrastructure and Systems must not jeopardise the fair, safe and productive technology environment used by TasNetworks' workforce, nor jeopardise TasNetworks' operations, assets and reputation.

3.1.3 TasNetworks' technology services, Infrastructure and Systems must not be used unlawfully or for an unlawful purpose.

3.1.4 Large data downloads or transmissions should be minimised to ensure the performance of technology resources for other Users is not adversely affected.

3.2. Access and Accounts

3.2.1 All Users are entitled to access TasNetworks' technology services, Infrastructure and Systems at a level appropriate to their position and role in accordance with this policy and related procedures.

3.2.2 Some technology facilities provided for public community use do not require a unique account to enable access such as the TasNetworks public website.

3.2.3 Contractors, consultants and third-party operators to TasNetworks may be provided with access to TasNetworks' technology services, Infrastructure and Systems in accordance with this policy and related procedures, where the use of those facilities and services is necessary for them to undertake their tasks for TasNetworks.

3.2.4 TasNetworks may impose restrictions on the use of TasNetworks' technology services, Infrastructure and Systems (including print, file storage, email and internet download) and will revise them as necessary.

3.2.5 When account holders no longer require or are no longer authorised to have access to TasNetworks' technology services, Infrastructure and Systems, their accounts will be disabled for a set period but remain accessible to the designated TasNetworks authorised administrators, including but not limited to, an ex-employee's leader and service providers who may have to dispose of data or documents in the account, and then be deleted.

3.2.6 Account holders may have their access to TasNetworks' technology services, Infrastructure and Systems suspended immediately where there is a suspected breach of this or other related policy.

3.2.7 Account holders who have multiple relationships with TasNetworks who cease only one of their relationships will only have the access related to the terminating relationship removed.

3.2.8 Telephone logs, call records or itemised bills for TasNetworks owned mobile devices may be made available to Leaders.

3.2.9 Access rights to User files, mail boxes and logs are restricted to those with responsibility for administering the particular Systems. Access by other personnel is only available with approval of the General Manager – People and Performance or the CEO. Upon departure of a User, such access to other Users may be granted by the User's immediate Leader or supervisor.

3.2.10 Access to mobile device GPS data will only be provided to authorised Users for security, safety and/ or business related purposes.

3.3. Security of Information Technology Facilities and Services

3.3.1 TasNetworks will take all reasonable steps to protect its technology services, Infrastructure and Systems from unauthorised and unacceptable use.

3.3.2 The Information Technology Leader and their direct reports are responsible for the implementation and management of this Policy in relation to TasNetworks' technology services, Infrastructure and Systems, within their remit.

3.3.3 To preserve TasNetworks' standard operating environment and ensure compliance with licensing obligations, Users must not modify the standard configuration of any of TasNetworks' technology services, Infrastructure and Systems without the appropriate authorisation from the Information Technology Leader or their delegated authority.

3.3.4 Users must never install or use unlicensed or malicious software on TasNetworks' technology services, Infrastructure and Systems and must not connect unapproved networking devices to technology Infrastructure.

3.3.5 Users of TasNetworks' technology services, Infrastructure and Systems must not circumvent TasNetworks' authorised internet connections or subvert its IT security measures.

3.3.6 All TasNetworks' IT hardware, especially portable devices, must be kept secured at all times against damage, misuse, loss or theft. In addition, hardware and software containing sensitive information or data must be protected with appropriate security measures such as passwords and encryption. Refer to the Information and Communications Security Policy and the Mobile Devices Policy for further guidance.

3.3.7 Under the Information Management Policy all business related information must also be saved in the designated information management system, unless stored in an approved file share environment. Users must not store or backup confidential or valuable data with externally hosted services other than where provided through and approved by the Information Technology Leader or approved delegate.

3.3.8 TasNetworks' IT hardware that becomes obsolete or is replaced with a more current model must be returned to the Service Delivery Team who will dispose of it in line with approved disposal procedures.

3.3.9 All technology hardware or Infrastructure that is not in use must be returned to the Service Delivery Team.

3.3.10 All Users must:

a) not use their access to TasNetworks' technology services, Infrastructure and Systems to gain any inappropriate personal advantage;

b) not – outside of their official role - manipulate TasNetworks' data without authorisation; and

c) maintain the confidentiality of any personal or confidential information accessed via TasNetworks' technology services, Infrastructure and Systems. Refer to the *Privacy Policy* for further details.

3.4. User Responsibilities

3.4.1 It is a condition of use of TasNetworks' technology services, Infrastructure and Systems that this Policy, particularly the principles of acceptable and unacceptable use, and its associated Policies and Procedures must be complied with.

3.4.2 Users may only use TasNetworks' technology services, Infrastructure and Systems as reasonably necessary to perform the duties of their position. For example, a User must not use TasNetworks' technology services, Infrastructure and Systems to access Confidential Information of TasNetworks that is not relevant to the performance of the duties of their position, or to share Confidential Information of TasNetworks with external or internal persons except where authorised for the performance of their duties.

3.4.3 All account holders are responsible for all activity initiated from their account, must only access TasNetworks' technology services, Infrastructure and Systems using their own account, and must ensure that their passwords are securely stored. Users are responsible for the following:

a) all activities that originate from their account;

b) all information sent from, intentionally requested, solicited or viewed from their account; and

c) information placed on a computer using their account.

3.4.4 Revealing a User account and/or password to others or allowing unsupervised use of a User account or devices by others is not permitted.

3.4.5 Providing information about, or lists of, TasNetworks' employees, customers or suppliers to parties outside TasNetworks outside of normal business requirements is not permitted.

3.4.6 Circumventing User authentication or security of any host, network or account is not permitted.

3.4.7 Users of TasNetworks' technology services, Infrastructure and Systems provided by a third-party vendor on TasNetworks' behalf must comply with any terms and conditions issued by that third-party provider as well as TasNetworks' policies and procedures. Users will be advised of any third party requirements when they are provided with access to the third party provided system.

3.4.8 Users of TasNetworks' technology services, Infrastructure and Systems must not create, send, store, upload, access, use, solicit, publish or link to:

a) Offensive, obscene, profane or indecent images or material;

b) Material likely to cause annoyance, inconvenience or distress to some individuals or cultures;

c) Discriminating or sexually harassing material or messages that create an intimidating or hostile work environment for others;

d) Defamatory material or material that makes misrepresentations or could otherwise be construed as misleading1;

e) Material that infringes the intellectual property (including copyright) of another person or organisation, including video and music files;

f) Malicious software such as viruses, worms or address-harvesting software;

g) Making fraudulent offers of products, items, or services originating from any TasNetworks account; or

[1] Excludes sending material internally for the purpose of obtaining legal advice

h) Material deemed as 'illegal content', which may include:

I. hate incitement;

II. child abuse content;

III. terrorism related content; or

IV. privacy-invading material, among others.

3.4.9 TasNetworks’ technology services, Infrastructure and Systems must not be used in the regular conduct of personal business or unauthorised commercial activities. Minor incidental personal use of TasNetworks’ telephones is permitted.

3.4.10 Employees are obligated to use the TasNetworks email signature style provided and endorsed by the TasNetworks communications team on all email messages sent, in accordance with policy guidelines.

3.4.11 Peer-to-peer software (a distributed application architecture that partitions tasks or workloads among peers and generally requires identical access to all others where participants are equally privileged) must only be used for lawful purposes authorised by the Information Technology Leader or their designated authority.

3.4.12 Employees are restricted from using non-work related entertainment related streaming services such as Netflix, ABC iView or other media streaming services on the corporate WiFi network due to potential impact on business operations.

3.4.13 All TasNetworks information must be communicated using TasNetworks approved communication tools including Microsoft Skype for Business (formerly known as Lync). Users are not permitted to use third party messaging applications unless authorised by the Information Technology Leader or delegated authority.

3.4.14 Users must ensure that they do not leave TasNetworks’ technology services, Infrastructure and Systems unsecured or open to unauthorised access/use.

3.4.15 Any observed security weakness in, or threat to, TasNetworks’ technology services, Infrastructure and Systems and/or any known or suspected breach of this Policy and its associated Policies and Procedures must be reported as soon as practicable to the IT Infrastructure Team Leader and/or IT Service Desk.

3.4.16 Where use of TasNetworks’ technology services, Infrastructure and Systems would ordinarily breach this Policy, but the use forms a legitimate part of the User's role at TasNetworks, an exemption may be granted from compliance with this Policy by the Information Technology Leader.

3.4.17 Users must be aware that email is a very common method of security threats, and as such Users must take care when reading emails from external sources:

a) Users should carefully check that the From and Reply-To addresses match the email address of the person the email appears to be from;

b) Users should be alert to an email that is prompting them to act urgently. Users should not act on any email which is unusual or out of the ordinary;

c) Users should only open attachments from people who are trusted and from whom an email would be expected;

d) Users should avoid clicking through website links contained in email. Where there is cause for suspicion the known site address should be typed into the browser or a search for the website undertaken.

3.4.18 Software must not be downloaded and installed from the internet. Software should only be installed if the User is authorised to do so and has been authorised by the IT Service Delivery Team Leader or IT Infrastructure Team Leader to download the software from a trustworthy source.

3.5. Email and Communications

In relation to email and other communications, the following are NOT permitted:

3.5.1 The use of global e-mail messages for non-urgent business. The appropriate method of communication for non-urgent messages to the entire business is via the internal Intranet site, The Zone. Global messages are strictly limited to urgent company-wide messages and require the approval of the internal communications team. Exceptions to this policy statement may be provided by written approval from General Managers or the Information Technology Leader;

3.5.2 Sending unsolicited email messages, including the sending of "junk mail", “chain letters” or other advertising material to individuals or groups who did not specifically request such material (email spam - breaching the SPAM Act 2003);

3.5.3 Engaging in any form of harassment via email, telephone or text messaging, whether through language, frequency, or size of messages;

3.5.4 Unauthorised use, or forging, of email header or footer information; and

3.5.5 Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

3.6. Use of External Storage Devices (USBs, hard drives)

3.6.1 In using external storage devices on TasNetworks’ technology Infrastructure or Systems, Users must be aware and must make all reasonable efforts to ensure that Malicious software is not introduced to TasNetworks’ technology Infrastructure and Systems. Where practicable an external storage device required in the course of a User’s work for TasNetworks should be obtained from the IT Service Delivery Team.

3.6.2 Any external storage device found or provided by external parties should be checked and cleaned of any malicious software prior to connecting to TasNetworks’ Infrastructure and Systems. The IT Service Delivery team can assist with checking of these devices.

3.6.3 In storing documents or other information of TasNetworks on an external storage device, Users must ensure that they comply with TasNetworks’ Information Management Policy, including that all documents must be saved into the InfoZone.

4. Social Media Code of Conduct

4.1. Social Media Sites

TasNetworks has social media sites on Facebook (http://www.facebook.com/tasnetworks), Twitter (@TasNetworks), LinkedIn (http://www.linkedin.com/company/tas-networks) and YouTube (www.youtube.com/user/tasnetworks).

TasNetworks encourages employees to follow social media pages and engage and promote TasNetworks' content in accordance with this policy.

To share or promote TasNetworks' related content or activities on the TasNetworks social media sites, contact the Brand and Communications Team or email brandandcommunications@tasnetworks.com.au.

4.2. Social Media Code of Conduct Statement

4.2.1 When using social media Users must not engage in activity that may harm or tarnish the image, reputation and/or goodwill of TasNetworks.

4.2.2 When using social media, Users must not, expressly or implicitly, attribute personal statements, opinions or beliefs to TasNetworks. If it could be inferred, implied or understood that the person is representing TasNetworks, the person must clarify by stating that their comment/contribution is as a private individual and not as a representative of TasNetworks.

4.2.3 Users are prohibited from revealing TasNetworks' confidential or proprietary information, trade secrets, trademarks, logos, photos or any other material on social networks without expressed written permission from a General Manager and the Brand and Communications Team Leader.

4.2.4 Limited and occasional use of TasNetworks' Systems to engage in social media is permissible, provided that it is done in a professional and responsible manner, it is not detrimental to TasNetworks' best interests, and does not interfere with an employee's regular work duties.

4.2.5 TasNetworks may request the removal or modification of social media content if the content is in breach of this Policy or this Social Media Code of Conduct.

4.3. How can I be sure my conduct complies with the Social Media Code of Conduct?

While the Social Media Code of Conduct provides general guidance and minimum expectations regarding your conduct online, no code can cover every conceivable circumstance you may be faced with.

If you find yourself in a situation where you are unclear as to the correct action you may consider the following:

- Could what you are doing harm the reputation of TasNetworks?

- Are you disclosing any business material that you are not specifically authorised to disclose?
- Have you made it clear to others when your contribution is as a private individual and not as a representative of TasNetworks?
- Are you willing to defend what you post to your Leader? Would you be comfortable saying it to a stranger at a bus stop, or posting it on a public shop window?
- Are you behaving with integrity, respect and accountability?
- Consider whether you would be comfortable if your actions were reported in the media;
- Think about who will benefit –will it be fair to TasNetworks, the customer and yourself?

If you have doubts about the correct thing to do, you should seek advice from your Leader, the Brand and Communications Team or by emailing brandandcommunications@tasnetworks.com.au.

5. Monitoring of Technology Services

- TasNetworks will manage account holders' accounts, maintain a secure technology environment and keep Users informed of their responsibilities.
- TasNetworks reserves the right to investigate any and all aspects of its electronic information Systems and telecommunications services if it is suspected that any User of TasNetworks' technology services, Infrastructure and Systems is acting unlawfully or violating either this Policy or any other TasNetworks Policy.
- TasNetworks reserves the right to monitor, log, collect and analyse the activities of Users in their usage of TasNetworks' technology services, Infrastructure and Systems.
- TasNetworks may review personal posts to investigate fraud (for example claiming sick leave inappropriately etc).
- TasNetworks may take any action it considers necessary to remedy immediate threats to TasNetworks' technology Infrastructure or security, including suspending authorised accounts and/or disconnecting or disabling relevant technology services, Infrastructure and Systems or other equipment, with or without prior notice.
- TasNetworks reserves the right to carry out security audits on TasNetworks' technology services, Infrastructure and Systems.
- TasNetworks reserves the right to block or filter any network or communications traffic that potentially breaches this policy or is potentially illegal.

6. Roles and responsibilities

6.1. Chief Executive Officer

The Chief Executive Officer is responsible for approving and communicating this Policy.

6.2. TasNetworks Leadership Team (TLT)

Each General Manager is accountable for ensuring that this Policy is complied with throughout their group. All Users are expected to use TasNetworks' technology facilities and services responsibly and in accordance with this and other related policies, procedures and guidelines as advised from time to time.

6.3. Information Technology Administrators and Service Providers

Technology administrators, Leader and Users and their service providers are responsible for the provision and maintenance of TasNetworks' technology facilities, sites and services and for ensuring that their use does not present a threat or risk to TasNetworks, its interests, or its employees.

6.4. Information Technology Leader

The Information Technology Leader has responsibility for all decisions that affect the TasNetworks' technology services, Infrastructure and Systems and associated facilities (subject to the delegations framework). The Information Technology Leader may confer their authority to their direct reports on any matter concerning the company's technology facilities or services and the governance of policy or procedures that affect their remit.

6.5. Service Delivery Team Leader

The Service Delivery Team Leader is responsible for:

- developing;
- maintaining;
- monitoring; and
- ensuring effective operation of this Policy and any related procedures.

6.6. Business Owners

Business Owners are the Subject Matter Experts for specific applications approved for use by TasNetworks and their correct and authorised use within the business. Business Owners are responsible for the following:

- Requiring that all Users of approved applications and/or Systems under their remit have their account authorised in writing before access is enabled; and
- Accounts on Systems under their control conform to password guidelines.

7. References

Users are reminded that additional IT policies, procedures, standards and best practice guidelines must also be adhered to, as advised by TasNetworks from time to time.

These documents are available on the TasNetworks Intranet under Policies, and should be made available to all Customers and Contractors who are given access to TasNetworks internal IT Systems by those requesting the access.
Link to these documents:
http://businesszone.tnad.tasnetworks.com.au/policies/Pages/Policies%20and%20Procedures.aspx
Users must read, understand and comply with the following procedures, policies, and others as issued from time to time:

- Information and Communications Security Policy
- Mobile Devices Policy
- Code of Conduct
- Alcohol and Other Drugs Procedure
- Information Management Policy
- Right to Information Policy
- Risk Management Policy
- Fraud and Corruption Policy

7.1. Compliance

Breaches of this policy will be treated seriously and may if necessary result in disciplinary action being undertaken. Depending on the circumstances of the case, this may include an apology, counselling, training, demotion or termination of employment. Behaviour that is not a breach of this Policy may still be found to be inappropriate or unreasonable. For example, it may be a breach of the TasNetworks Code of Conduct. In this instance, disciplinary action may still result.

Public Interest Disclosure Statement (“Whistleblowers”)

If an individual is concerned about consequences associated with reporting a serious breach of this Policy, that individual should refer to the Public Interest Disclosure (Whistleblowers) Policy, available on the Zone or talk to their Leader.

7.2. Definitions

Term	Definition
Business Owner	Defined in the body of the Policy.
Confidential Information	Confidential Information is any information: a) disclosed to a User by or on behalf of TasNetworks; or b) which comes into the User's possession, or is generated by the User in the course of performing their position, whether or not the information was originally supplied by TasNetworks, but does not include information in the public domain other than by a breach by the User of their obligations of confidentiality to TasNetworks. Confidential Information includes information which is intended for a restricted audience within TasNetworks (e.g. TLT, the Board or an employee file), and so should only be accessed by the intended audience and not the broader business.
Infrastructure	Infrastructure means the mechanical, magnetic, electronic, and electrical devices and associated information technology equipment forming or capable of forming the physical components of a computer or a computer system, including servers, power units, power cords, disk storage units, tape storage units, data cables, cabinets, enclosures, racks, shelves, consoles, monitors, keyboards, pointing devices, controllers, switches, gateways, routers, hubs, firewalls, security appliances, disk media, tape media, printers, scanners and cameras.
Service Delivery Team Leader	Defined in the body of the Policy.
Systems	Computer programs, including software, source and object code and operating systems.
User	Defined in the body of the Policy.
User Account	The login and password setup for a user to access a network, computer system, application or set of applications.

8. Need to know more or have a question?

All Team Members will have access to this policy and underpinning policies on The Zone. Support and further information is available from your Leader, People & Performance Partner or People Direct.

9. Administration of this Policy

This policy is administered by Information Technology and will be reviewed on an annual basis and updated where applicable.

Reviews are scheduled to:

- examine the policy's effectiveness as demonstrated by the nature, number and impact of recorded security incidents;
- consider the cost and impact of controls on business efficiency; and
- review the effects of technology changes.

Ad hoc reviews may take place in response to any changes affecting risk levels e.g. Significant security incidents, new vulnerabilities or changes to the organisational or technical Infrastructure.

Authorisations		
Action	**Name**	**Date**
Prepared by	IT Integration Program	
Reviewed by	GM Finance and Business Services	
Authorised by	Chief Executive Officer	

Document control				
Date	**Version**	**Description**	**Author**	**Approved by**
16 May 2014	0.1	Draft for Stakeholder review prior to issue for feedback.	John Mazengarb	
20 May 2014	0.2	Updates from drafting review, edits and clarifications	Josh Luttrell / John Mazengarb	
27 May 2014	0.3	Updated for Stakeholder feedback	John Mazengarb	
2 June 2014	0.4	Remove mark-up edits following Information Technology Leader sign off on draft	John Mazengarb	Melissa Lukianenko
June 2014	1.0	Version for approval	John Mazengarb	Chief Executive Officer
August 2014	1.1	Additional Social Media Code of Conduct	Allison Winter Jacqueline Collis Steve Mason	Chief Executive Officer
November	1.2	Minor edits to Social Media	Jacqueline	

2014		Conduct to remove duplication and improve clarity	Collis Steve Mason	
3 March 2015	1.3	Minor edits made	Alec Eiszele, Legal Services Team	Endorsed by Ross Burridge, GM Finance & Business Services
25 March 2015	2.0	Version published on Zone	Sarah Pidgeon	
25 March 2015	3.0	Version published on Zone	Sarah Pidgeon	Minor amendments
February 2017	4.0	Document updates to reflect new ICT strategy and best practices	Steve Mason	
July 2017	4.1	Updates from Legal and CEO review	Steve Mason	Corrections and minor amendments
July 2017	5.0	Revision for publication	Sarah Pidgeon	Chief Executive Officer