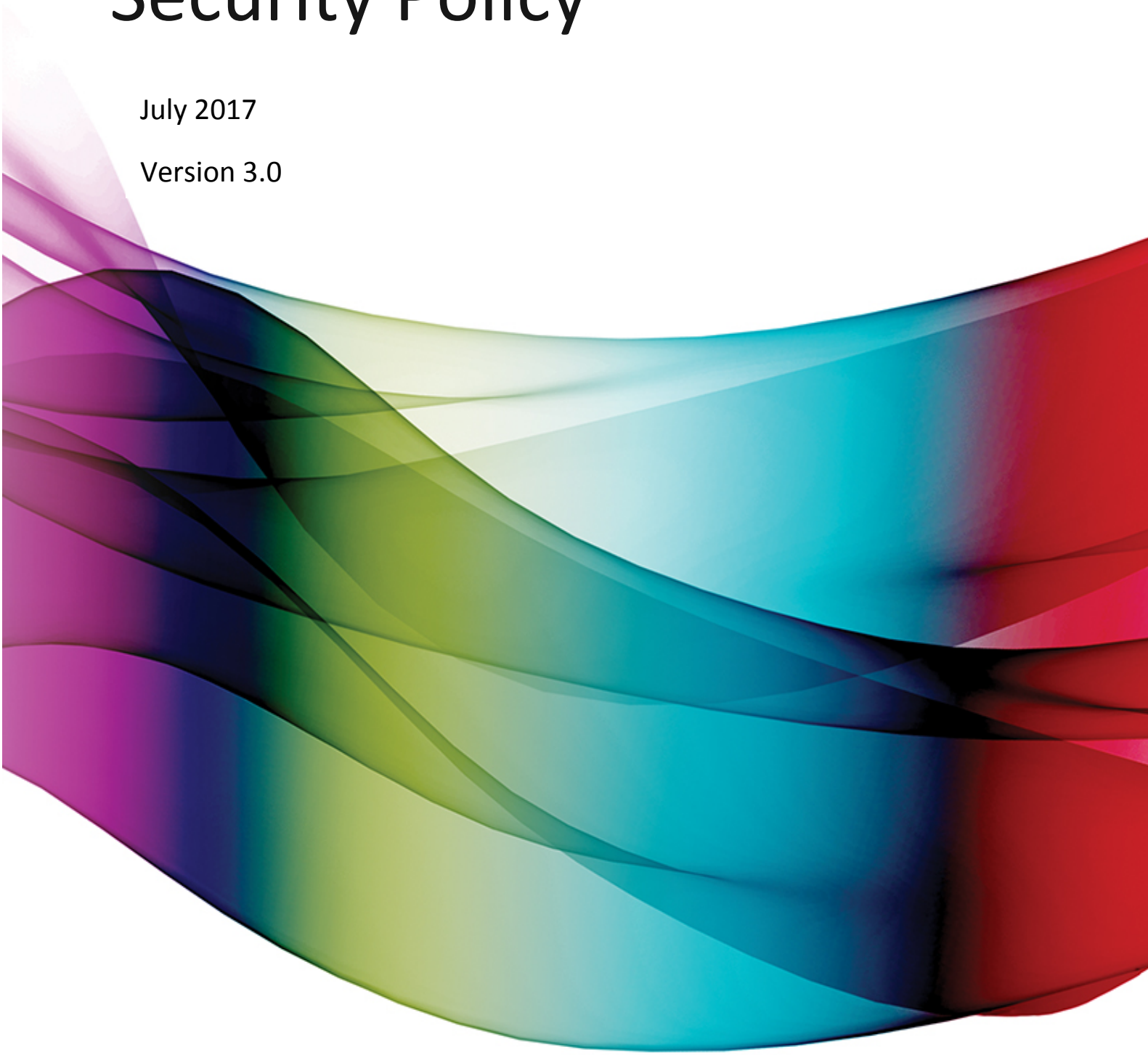
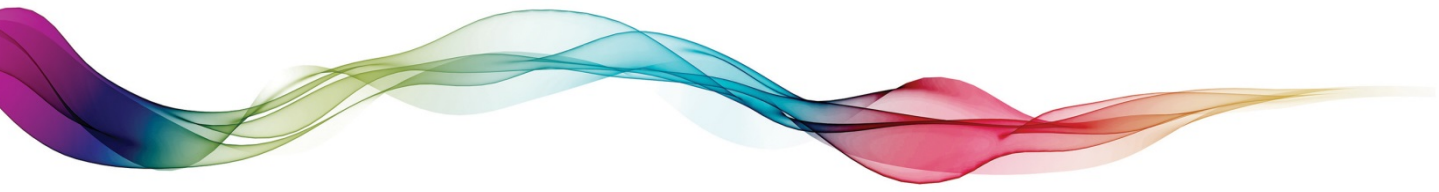
Information and Communications – Security Policy

July 2017

Version 3.0



Contents



1. Introduction and Purpose

This policy sets out TasNetworks' requirements for managing security, identity and access management of TasNetworks' technology services, Infrastructure and Systems that are appropriate for the organisation and meet the compliance or regulatory needs of the market in which TasNetworks operates. This includes policy for identification, authentication and authorisation of individuals or groups for access to TasNetworks' technology services, Infrastructure and Systems.

This Security Policy is required to ensure:

- protection of records, data and information;
- control of physical access to assets, including sites of TasNetworks' technology operations; and
- control of information and communications technology owned or operated by TasNetworks.

2. Who does this Policy apply to?

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

- team members (employees);
- 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.

The policy applies to both logical and physical access control mechanisms.

If specific TasNetworks Systems or sites require measures different from those detailed in this policy document, those variations will be documented in the appropriate additional TasNetworks procedural documentation.

Technology Infrastructure and Systems include both operational (field based) and corporate (office based) resources. These include:

- data communications equipment e.g. switches, routers, wireless network equipment;
- software;
- data storage equipment and information management Systems;
- power and network cabling;
- computers (desktop, laptop, server and associated accessories);
- printers, scanners, faxes and photocopiers;
- business telephones, mobile phones and Personal Digital Assistants (PDA), tablets; and
- all devices connected to TasNetworks' IT networks.

Any resources exempted from this policy will be authorised by the Information Technology Leader and a register of approved exemptions maintained.

3. Policy Detail

3.1. Principle of Least Privilege

3.1.1 The principle of least privilege requires that in a particular layer of a computing environment, every module (such as a process, a User, or a program) must be able to access only the information and resources that are necessary for its legitimate purpose ("Principle of Least Privilege").

3.1.2 The Principle of Least Privilege applies to all logical and physical access and control mechanisms for all technology services, Infrastructure and Systems and associated facilities.

3.2. User Identification

3.2.1 All Users must be uniquely identifiable and will be issued a unique user-id.

3.2.2 Generic or shared user-ids are not permitted for accessing TasNetworks' Systems. Exceptions for restricted access accounts on kiosk type devices require written approval from the Information Technology Leader or approved delegate.

3.2.3 Where a User performs multiple roles with different levels of access (such as a User that performs general office functions as well as system administration functions) they will have separate user-ids for the separate roles.

3.2.4 Users will not use a higher privileged account when that higher level of access is not required.

3.2.5 Default accounts that are installed as part of hardware, operating system or application installation will be removed or disabled on all TasNetworks Systems. Default accounts such as 'guest' that may still be required or cannot be removed will have their password changed from the default.

3.2.6 Service accounts used for application processes that require non-expiring passwords will not be used for any login purposes other than to run application processes. Where possible service accounts will have interactive login capability disabled.

3.2.7 Users accessing TasNetworks' Systems remotely (external to the TasNetworks IT network) will be required to provide multiple factors of authentication.

3.3. User Authentication

3.3.1 All users must be authenticated via a user-id and password or pincode / passcode on each occasion that access is granted.

3.3.2 TasNetworks will implement procedures to monitor and maintain user access.

3.3.3 The IT Service Desk, under the direction of the Information Technology Leader or approved delegate, will be solely responsible for:

a) creating, maintaining, restricting, disabling and deleting User accounts, groups, passwords and other items used for user authentication;

b) resetting passwords in the case that they cannot be reset by the User;

c) performing emergency disablement of User accounts immediately where requested by an authorised person (for example, where an immediate dismissal occurs); and

d) identifying and disabling inactive accounts.

3.4. Password Policy

3.4.1 Passwords are required for all User access to all technology services, Infrastructure and Systems.

3.4.2 Procedures and guidelines for creation, use and maintenance of passwords are the responsibility of the Information Technology Leader.

3.4.3 To maintain IT network security, User passwords must be changed every 90 days, but cannot be changed again within 3 days. There is a password complexity requirement for all TasNetworks users when prompted to renew their network password. This may change from time to time and is available on the Zone.

3.5. User Authorisation

3.5.1 All Users requiring access to TasNetworks' technology services, Infrastructure and Systems as well as the associated facilities will have the access approved by their Leader and requested in accordance with the agreed TasNetworks IT Service Desk procedure, prior to access being granted.

3.5.2 Authorisation levels for all Users will be granted on the Principle of Least Privilege.

3.5.3 System Administrators of TasNetworks' business Systems and applications must hold a formal approval from the IT Infrastructure Team Leader or delegate for these roles for each system or application that they administer.

3.5.4 The IT Service Desk, under the direction of the Information Technology Leader or approved delegate, will be solely responsible for creating, maintaining and deleting access privileges for software, directories, data, common middleware, database management Systems and other access profiles for all Users. The exception to this is SAP where the Security Architect role will advise the service provider of SAP on user access privileges for all SAP components.

3.6. Privileged Access

3.6.1 Privileged Access is access which can give a User:

a) the ability to change key system configurations;

b) the ability to change system control parameters;

c) access to audit, logs and security monitoring information;

d) the ability to circumvent security measures;

e) database level access including the ability to view, change or delete database structures, controls or data;

f) access to data, files and accounts used by other Users, including backups and media; or

g) special access for troubleshooting the system.

3.6.2 Privileged Access to TasNetworks' technology services, Infrastructure and Systems will be:

a) restricted to key authorised personnel only;

b) based on a secure logon, and additional authentication controls;

c) restricted such that there is no access to commercial or client information, except as required in the authorised course of the execution of duties;

d) logged; and

e) monitored for indications of malicious activity.

3.6.3 Privileged Access to TasNetworks' technology services, Infrastructure and Systems will require written authorisation by the Information Technology Leader or higher level position prior to the access being granted.

3.6.4 Processes to manage Privileged Access to technology resources will be documented and followed by the business and the technology personnel (e.g. TasNetworks' IT Service Desk and system administrators).

3.6.5 Information related to Privileged Access to TasNetworks' technology services, Infrastructure and Systems and the access that is given will be contained in an Access Register.

3.6.6 Privileged accounts will be reviewed by the General Manager or approved delegate, for their area of responsibility, at least every 6 months. The review is to ensure that Users do not have more privileges than required by their authorised role, and that redundant User accounts are removed from both the Register and the system.

3.7. Physical Access

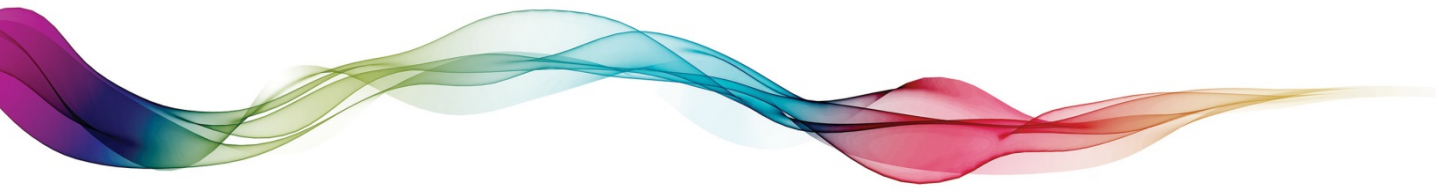
3.7.1 Physical access to TasNetworks' technology services, Infrastructure and Systems and associated facilities will be granted on the Principle of Least Privilege. Physical access includes access to data centres, server rooms, offices, cabinetry, and other locations housing TasNetworks' technology Infrastructure, Systems and networks.

3.7.2 Network and information storage servers will be housed in a physically secure location. Secure areas will be protected by appropriate entry controls to ensure that only authorised personnel can gain access.

3.7.3 Physical security will be enforced by electronic access cards. Where this is not suitable keyed access and log books will be used.

3.7.4 All electronically controlled physical access (ingress and egress) will be logged and monitored.

3.7.5 The authorisation process for physical access to TasNetworks' technology services, Infrastructure and Systems and associated facilities including data centres covered by this policy



will be established under the guidance of the Information Technology Leader or approved delegate.

3.8. Visitor Access to TasNetworks' Technology Facilities

3.8.1 Visitors to TasNetworks' technology facilities, sites and premises must sign a visitor book and be escorted at all times by an employee, or an approved contractor or consultant, authorised by the Leader of the area.

3.8.2 TasNetworks employees are encouraged to question visitors to their area if the person is unknown to them and/or unescorted.

3.8.3 Users must be alert for "tailgating" and other illegal entry activities to TasNetworks' technology facilities, sites and premises, including non-technology sites such as regional offices, depots and substations, by persons unknown to them. Such activities must be reported to Security or their Leader immediately.

3.9. Web Access

3.9.1 Web access by Users will be controlled to reduce the security risks associated with this service. Web proxy servers will have the following:

a) Malicious software detection and protection for all devices retrieving information;

b) Detection and protection Systems for malicious software in transit;

c) Filtering mechanisms in place to manage content; and

d) Separation and controls between servers accessing internet content and customer networks.

3.10. Antivirus Software

3.10.1 Antivirus software will be maintained on all TasNetworks devices capable of supporting this software.

3.10.2 No User may uninstall, change, alter, bypass or otherwise modify, prevent or inhibit the operation of antivirus software.

3.10.3 Antivirus software and virus definitions will be kept up to date at all times.

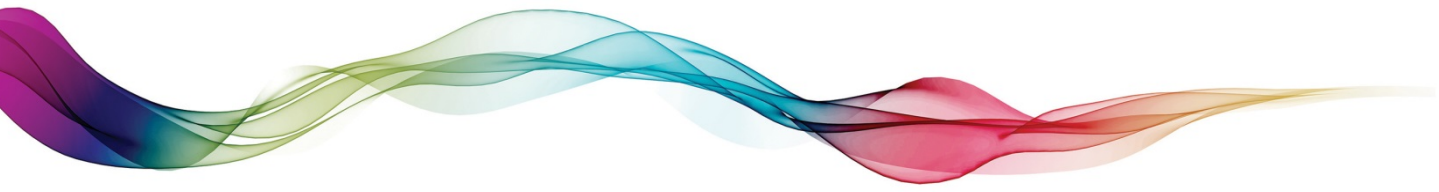
3.11. Security

3.11.1 TasNetworks' desktops, laptops, tablets and smart phones (computers) will be configured with a screen or session lock. Any exceptions for operational reasons must be approved in writing by the Information Technology Leader.

3.11.2 Users will not leave a device unattended without a screen or session lock activated.

3.11.3 TasNetworks' technology Infrastructure will be sited to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.

3.11.4 TasNetworks' information should not be stored by Users in personal storage or collaboration facilities nor sent via personal email accounts.



3.12. Monitoring and Control

3.12.1 Any person who becomes aware of any loss, compromise, or possible compromise of information, or any other incident which has technology security implications, must immediately inform their Leader and the IT Service Desk immediately.

3.12.2 The Information Technology Team, under the direction of the Information Technology Leader or approved delegate, will be responsible for ensuring the physical and logical security and control of access to TasNetworks' technology services, Infrastructure and Systems, and will review and monitor the levels of access for Users performing development, enhancement, maintenance, support and operations functions in those environments.

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

3.12.4 User access and authentication for all technology services, Infrastructure and Systems will be logged and such logs will be subject to Privileged Access controls.

3.12.5 All User authentication and access will be monitored and assessed for:

a) unusual or suspicious activity;

b) unauthorised use or access to sensitive data; and

c) violations of this Policy.

3.12.6 The Information Technology Team will conduct information security audits at least annually for the TasNetworks technology services, Infrastructure and Systems, and will produce a report for each audit detailing the findings of the audit, including any material non-compliance with information security policies and procedures. The Information Technology Team will promptly action and resolve findings from internal and external information security audits to ensure the ongoing compliance with this Policy.

3.13. Use of TasNetworks' Technology Services and Access to Information

3.13.1 Users must only use TasNetworks' technology services, Infrastructure and Systems as reasonably necessary to perform the duties of their position. If a User has inappropriate access to a service or system (e.g. a system or service that is not relevant to their role, or which gives them access to Confidential Information for which they are not the intended audience), the User must advise their Leader and the IT Services Desk and must not continue the inappropriate access.

3.13.2 Users must maintain the security and confidentiality of TasNetworks' Confidential Information at all times. This includes:

a) complying with all technology security requirements in this Policy and related policies;

b) only accessing and using the Confidential Information of TasNetworks as reasonably necessary to perform the duties of their position, and ensuring that the Confidential Information remains secure at all times (this includes being secure from inappropriate access from both external and internal parties); and

c) reporting any breaches of security, or inappropriate access, to their Leader.

4. Roles and Responsibilities

4.1. Chief Executive Officer

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

4.2. TasNetworks Leadership Team (TLT)

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

4.3. Information Technology Administrators and Service Providers

Technology administrators, Leaders 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.

4.4. Information Technology Leader

The Information Technology Leader has ultimate responsibility for all decisions that affect TasNetworks' technology services, Infrastructure and Systems and associated facilities. The Information Technology Leader may confer their authority to their direct reports on any matter concerning TasNetworks' technology facilities or services and the governance of policy or procedures located on the Zone under Policies and Procedures that affect their remit.

4.5. Information Technology Infrastructure Team Leader

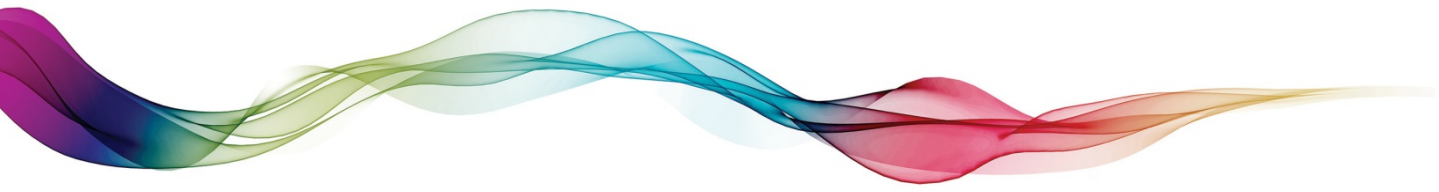
The IT Infrastructure Team Leader is responsible for:

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

4.6. Business Owners

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

- Requiring that all Users of 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.



4.7. Security Architect

Position responsible for security of workflows within SAP and Enterprise security governance across TasNetworks technology, Infrastructure and Systems.

5. 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 policies and procedures are available on the Zone here:

http://businesszone.tnad.tasnetworks.com.au/policies/Pages/Policies%20and%20Procedures.aspx

Users must read, understand and comply with the following policies, and others as issued from time to time:

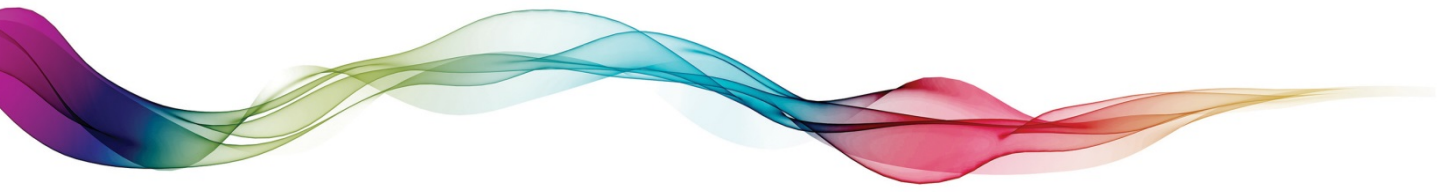
- Acceptable use of Technology Services Policy
- Mobile Devices Policy
- Alcohol and Other Drug Procedure
- Information Management Policy
- Right to Information Policy
- Risk Management Policy
- Fraud and Corruption Policy
- Privacy Policy

5.1. 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.



5.2. Definitions

Term	Definition
Business Owner	Defined in 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.
Systems	Computer programs, including software, source and object code and operating systems.
User	Defined in 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.

6. 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.

7. Administration of this Policy

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

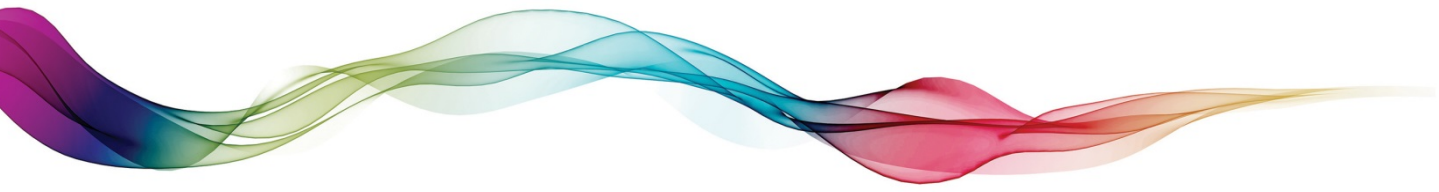
Reviews are scheduled to:

- 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	Updates for Stakeholder feedback	John Mazengarb	
30 May 2014	0.4	Additional feedback edits from Protection & Control Team	John Mazengarb	
2 June 2014	0.5	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
February 2017	2.0	Document updates to reflect new ICT strategy and best practices	Steve Mason	
July 2017	2.1	Corrections and minor	Steve Mason	Chief Executive Officer



		amendments after Legal and CEO review		
July 2017	3.0	Revision for publication	Steve Mason	Chief Executive Officer