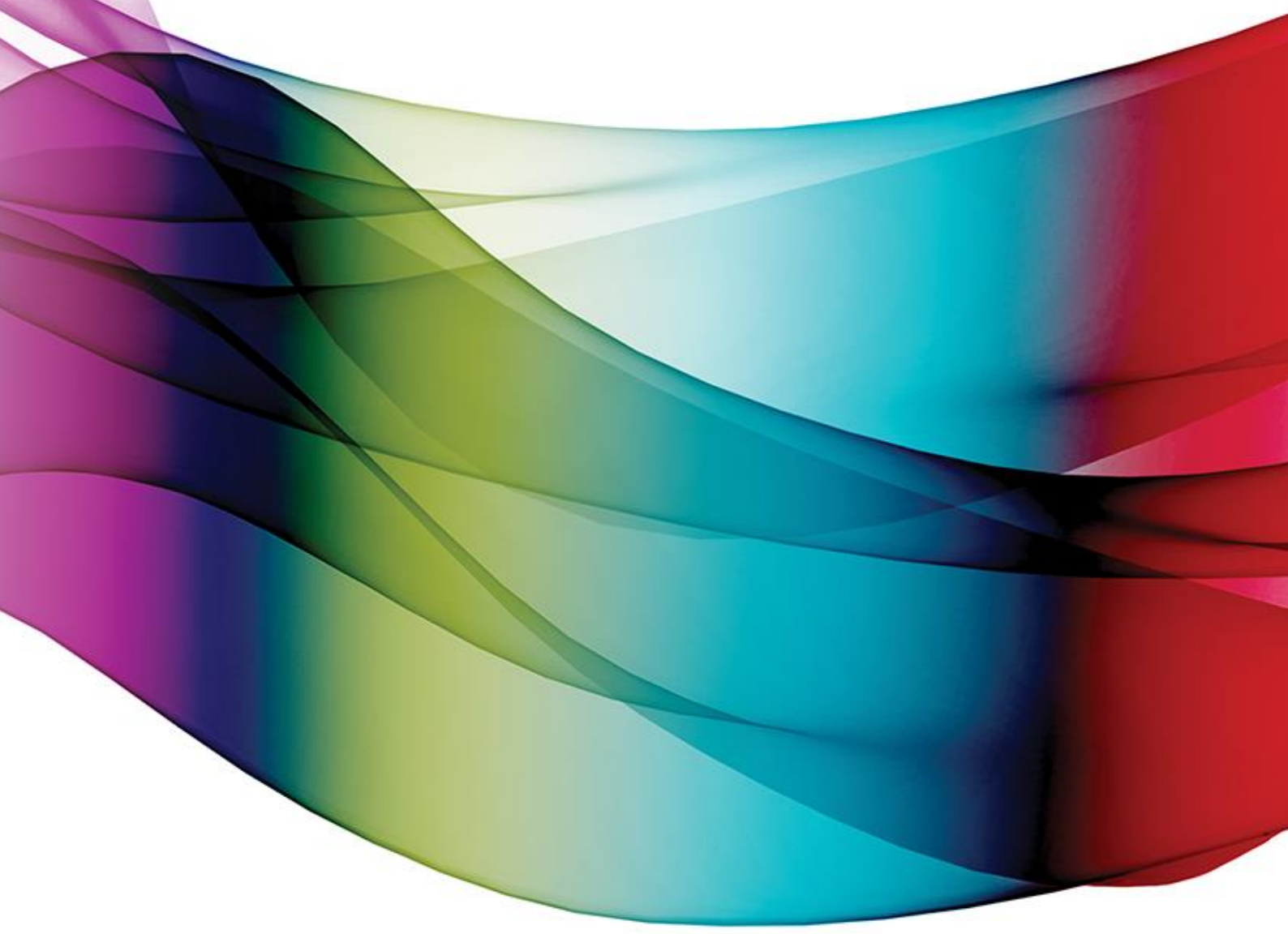
Mobile Devices, Wireless Service and Remote Access Policy

July 2017

Version #3



Contents

1. Introduction and Purpose

Mobile devices and wireless access is becoming a common and cost effective tool for information management and communication in the community and within business. In addition to increased prevalence of mobile devices, there is an increase in requests by TasNetworks workers and contractors to connect their own devices (Bring Your Own Device - BYOD) to TasNetworks equipment and networks.

TasNetworks recognises that these emerging mobility technologies can improve the way TasNetworks conducts business.

Greater security measures are required to mitigate the increased security risk from wireless access and the potential for business data to reside on mobile devices.

The purpose of this policy is to provide directives on the terms of use of mobile devices and wireless and remote access within the TasNetworks environment so that:

- systems and data are protected from unauthorised access, use or disclosure;
- the correct processes and procedures are followed when utilising mobile computing devices and technologies;
- TasNetworks team members are aware of their individual responsibilities in relation to the use and security of mobile devices for the transmission and storage of information and access to TasNetworks' technology services, infrastructure and systems;
- TasNetworks team members are aware of their responsibilities in relation to access and use of the wireless network in relation to TasNetworks applications and data; and
- guests and contractors (including employees of vendors) are aware of their obligations, responsibilities and the acceptable use of the wireless network infrastructure.

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
- visitors
- customers
- contracted third parties (vendors) and their staff or contractors.

Hereafter known as "**Users**".

This policy applies to the following equipment:

- TasNetworks owned mobile devices;
- Personal Devices utilised by Users for work associated with TasNetworks; and

Personal Devices utilised by Users accessing the TasNetworks network for private or personal use.

3. The Policy

3.1. Use of TasNetworks Owned Mobile Devices

3.1.1 All use of TasNetworks owned mobile devices for both work use and personal use, must be in accordance with this Policy and the Acceptable Use of Technology Services Policy.

3.1.2 Users are responsible for ensuring TasNetworks owned mobile devices are not accessed by persons that are not authorised by TasNetworks.

3.1.3 Personal use of TasNetworks owned mobile devices is limited to persons authorised by TasNetworks only. Shared use, lending or otherwise providing access to such devices by non-authorised persons is not permitted.

3.1.4 All use of TasNetworks owned devices on TasNetworks' technology services, infrastructure and systems for both work use and personal use, must be in accordance with the Acceptable Use of Technology Services Policy.

3.1.5 Users leaving TasNetworks are required to return TasNetworks' devices without any inhibiting software or configuration such as activation lock, time-bomb software, encryption or apps store/cloud passwords that prevents the device from being re-used by another employee.

3.1.6 Users must not tamper with corporate provided devices such as 'jail-breaking' or 'rooting' their mobile devices. Devices that are identified as having been Jail-broken or Rooted will be prevented from accessing TasNetworks facilities.

3.1.7 TasNetworks owned devices are locked to the TasNetworks chosen network provider. Transfer of such devices to other carriers will only be considered where a pressing business need is identified.

3.1.8 Users will not store data or information on TasNetworks devices that infringes copyright laws.

3.1.9 Data usage on TasNetworks devices is subject to periodic review. Ongoing excess usage charges more than 3GB/month may be investigated and additional costs passed on to the user of the device.

3.2. Use of Personal Devices

3.2.1 Users require written approval to connect Personal Devices to TasNetworks' technology services, infrastructure and systems, which will only be given by TasNetworks on the User's acceptance and implementation of the access conditions in this Policy.

3.2.2 By connecting Personal Devices to TasNetworks' technology services, infrastructure and systems, TasNetworks' network, systems or infrastructure Users accept the conditions of this Policy and access conditions contained herein.

3.2.3 The use of Personal Devices is subject to TasNetworks having the ability to install security, remote access, virtualisation or other software on the User's device. Such software may be secured with a password or pin code that is not made available to the User.

3.2.4 On acceptance and implementation of TasNetworks' access conditions, Users may be permitted to connect Personal Devices to TasNetworks' technology services, infrastructure and systems for the express purpose of accessing or using business applications, data or services for work purposes only. Such access may include:

a) receiving email, contact and calendar updates and using TasNetworks remote access to access these systems

b) accessing or using company licensed or owned software such as SAP Work Manager

c) accessing company data and data repositories such as SharePoint or the Zone

d) installing company licensed software and using that software to access company data, processes, intellectual property, confidential or sensitive information.

3.2.5 No company data, processes, intellectual property, confidential or sensitive information will be stored on any device in an insecure format and must be protected through application level security as well as device level security measures (ie pin code / password).

3.2.6 Users are responsible for ensuring TasNetworks' information on their Personal Devices is not accessed by persons that are not authorised by TasNetworks.

3.2.7 All use of Personal Devices on TasNetworks' technology services, infrastructure and systems for both work use and personal use, must be in accordance with the Acceptable Use of Technology Services Policy.

3.2.8 TasNetworks will maintain a list of all approved Personal Devices and related software. Personal Devices not on the list may not be used to connect to TasNetworks' technology services, infrastructure and systems. TasNetworks reserves the right to refuse connection of Personal Devices to the TasNetworks' technology services, infrastructure and systems.

3.2.9 TasNetworks will only grant access to networks, applications, databases or other services based on an approved need by that User. Not all applications or services will be made available to all Users with approved access for their Personal Devices.

3.2.10 Users may be required to install and configure TasNetworks' licensed software onto their Personal Devices, and do so at their own risk. Users will comply with any applicable licensing conditions as specified by the software vendor, and will not use that software in any manner that breeches those license conditions (including copying, modifying or distributing that software).

3.2.11 Users of Personal Devices connected to TasNetworks' technology services, infrastructure and systems acknowledge and agree that TasNetworks may remote wipe their device in the event of a security breach. While TasNetworks will endeavour to prevent the employee's personal data from being lost, in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.

3.2.12 Personal Devices must have a current and supported operating system and devices that use aged or unsupported platforms may not be approved for connection to TasNetworks' technology services, infrastructure and systems.

3.2.13 Users must not connect 'jail-broken' or 'rooted' mobile devices to the TasNetworks' network. Devices that are identified as having been Jail-broken or Rooted will be prevented from accessing TasNetworks technology services, infrastructure and systems.

3.2.14 Employees assume full liability for risks from using Personal Devices on TasNetworks' technology services, infrastructure and systems and release TasNetworks from all liability in connection with their use, including loss of personal data should TasNetworks wipe a device.

3.2.15 TasNetworks reserves the right to disconnect Personal Devices or disable services without notification.

3.2.16 Users who have their access cancelled for any reason, must uninstall any software, applications or services installed on their Personal Device, and delete any data or information that has been stored on the device as a result of connecting that device to TasNetworks' technology services, infrastructure and systems. TasNetworks reserves the right to remote wipe a Personal Device if the User refuses to comply with this Policy. This clause survives the termination of any employment or vendor contract with TasNetworks.

3.2.17 Prior to leaving TasNetworks, Users are responsible for retrieving any personal information or content from their TasNetworks provided device.

3.2.18 Users assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

3.3. Physical Security of Mobile Devices

The following must be observed when handling mobile computing devices – see also *Information and Communications Technology IT Security*:

3.3.1 All mobile devices that are used to access TasNetworks' technology services, infrastructure and systems must be appropriately secured at all times and secured by an access pin code or password and have encryption methods to secure the device.

3.3.2 Lost or stolen TasNetworks owned mobile devices and Personal Devices that access TasNetworks' technology services, infrastructure and systems must be reported to the IT Service Desk as soon as possible and no later than 24 hours after the User becomes aware that the device is lost or stolen.

3.4. Protection of Information on Mobile Devices

3.4.1 Users must securely protect information on mobile computing devices in accordance with TasNetworks Information and Communications Technology (ICT) Security and Access Policy.

3.4.2 In the event a TasNetworks owned mobile device or a Personal Device is lost or stolen, or the security of the device is believed to have been compromised, the device may be remotely wiped of all data and locked to prevent access by anyone other than TasNetworks. Remote wipe may destroy all data on the device, whether it is related to business or personal use.

3.4.3 Users of Personal Devices are to take full responsibility for backing up and securing all personal data, including photos and personal emails. Users acknowledge that such personal data may be destroyed by TasNetworks in the event that a remote wipe is undertaken on the device.

3.4.4 TasNetworks utilises certificates to restrict access to the corporate network. Users are required to accept TasNetworks' security certificates and profiles and are not permitted to inhibit, disable, tamper with or in any way limit security protocols, certificates or profiles on Personal Devices or TasNetworks owned devices.

3.4.5 TasNetworks reserves the right to repatriate a mobile device, whether corporately or personally owned, in the event of a legal action or legal dispute to access information specifically related to the legal dispute. As part of any investigation TasNetworks may elect to use forensic toolsets and the User will permit this to occur. The User will not deliberately tamper with any information relevant to the investigation nor restrict access thereto. The User must accept and will comply with this requirement as part of any Personal Device usage. TasNetworks will provide, up on request, a like device on loan during the period of investigation.

3.4.6 TasNetworks' information will remain the property of TasNetworks regardless of the device or software TasNetworks information is created or used on.

3.4.7 Personal information or content will remain the property of the User regardless of the device or software TasNetworks information is created or used on.

3.5. External Remote Access

This section applies to all Users who connect to the TasNetworks' technology services, infrastructure and systems from an external network such as the Internet.

3.5.1 Remote access to TasNetworks systems is provided to authorised Users and external support/consultant personnel to facilitate working from remote locations outside the TasNetworks network.

3.5.2 All Users that connect to the TasNetworks' technology services, infrastructure and systems from an external network must comply with the Acceptable Use of ICT Facilities and Services Policy.

3.5.3 Remote access is authorised to individual users, and not to groups of people. If multiple external people from the same organisation require access, then they must each apply and be approved separately.

3.5.4 A remote access session should only be active while the user is attending to the connected device. Users should terminate the session after completing work and/or before leaving the device unattended.

3.5.5 Where possible users must avoid use of public WiFi or untrusted networks to access TasNetworks systems including email. Alternatively, employees should use mobile device tethering to access TasNetworks information.

3.6. Support

3.6.1 TasNetworks will provide support services for the following:

a) TasNetworks owned devices, connection of those devices to the TasNetworks network and any approved applications and services on those devices.

b) TasNetworks software, applications, code or other functions that have been installed onto Personal Devices, provided those functions have been approved for use on that device.

3.6.2 TasNetworks will not provide support services for the following:

a) Any non-approved software installed onto a TasNetworks' owned device

b) Any software that is not used specifically to connect to or interact with TasNetworks' technology services, infrastructure and systems on Personal Devices, including operating systems.

3.6.3 All support is managed through standard Service Desk procedures. Users should contact the Service Desk for support.

3.6.4 During business hours, in-home support will only be provided to Users of TasNetworks owned devices in exceptional circumstances, where the user has exhausted all support avenues with their internet service provider and the approval of the Service Delivery Team Leader has been obtained. TasNetworks will not provide in-home support after hours.

3.6.5 TasNetworks will not provide in-home support for Personal Devices.

3.7. Safety Consideration

3.7.1 No mobile device shall be used in a way that presents a danger to the User, other people, plant, facilities or equipment.

3.7.2 The User will comply with all relevant OH&S policies, procedures, laws and regulations in relation to the safe operation of mobile devices. This includes not using devices whilst driving, confined spaces, operating equipment or near flammable substances.

4. Key Stakeholders 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 Service Providers

Technology administrators, managers 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 the business, its employees or their interests.

4.4. Information Technology Leader

The Information Technology Leader has ultimate responsibility for all decisions that affect the TasNetworks' technology services, infrastructure and systems and associated facilities. They have the right but not the obligation, to 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.

4.5. Service Delivery Team Leader

The Service Delivery Team Leader is responsible for:

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

4.6. Business Owners

Business Owners are the Subject Matter Expert repositories of knowledge 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.
- Accounts on systems under their control conform to password guidelines.

5. References

Individuals are reminded that additional ICT policies, procedures, standards and best practice guidelines must also be adhered to, where their employment indicates that the relevant policy is applicable to their employment responsibilities.

All staff, consultants, contractors and third party staff must read, understand and comply with the following ICT policies, and others as issued from time to time:

- Acceptable use of Technology Services Policy
- Information and Communications – IT Security Policy

Individuals will also be made aware of other relevant TasNetworks policies including the TasNetworks Code of Conduct at induction and are reminded that these policies have areas of overlap with ICT policies. The following policies are applicable and should be read and understood by all staff employed by TasNetworks. The list includes, but is not limited to, the following policies available on the Zone.

- Fit for Work Policy
- 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	Accountable for business ownership of ICT systems/applications/equipment
ICT	Includes all Information and Communications Technology equipment, sites, facilities and services contracted or purchased for use by TasNetworks
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	Position responsible for ensuring that this policy and any related procedures are adhered to with regard to access and use of TasNetworks ICT facilities and services
Systems	Computer programs, including software, source and object code and operating systems.
Staff	Permanent, part time and fixed term employees and other contractors and consultants engaged by TasNetworks
User	User means an individual who has access to and is authorised to use any technology service, infrastructure, system or associated facility.
User Account	The login and password setup for a user to access a network, computer system, application or set of applications.
Personal Devices	Non-TasNetworks owned mobile devices and computing devices

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
- 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	Ross Burridge, GM Finance and Business Services	
Authorised by	Lance Balcombe, CEO	

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 and John Mazengarb	
27 May 2014	0.3	Updates 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 2016	1.1	Updates	Alec Eiszele	
February 2017	2.0	Document updates to reflect new ICT strategy and best practices	Steve Mason	
July 2017	2.1	Updates from Legal and CEO review	Steve Mason	Chief Executive Officer
July 2017	3.0	Version for publication	Steve Mason	Chief Executive Officer