ICT AND INFORMATION MANAGEMENT

Bring Your Own Device (BYOD) Policy

Effective date: 15/01/2013 **Version: 1.8**

IMP/2012/5093

1. Purpose

This policy defines the acceptable practices, responsibilities, and commitment requirements for the use of personally owned mobile devices (known as Bring Your Own Device or BYOD) that are authorised to connect to Information and Technology Partners (ITP) managed networks and services.

2. Scope

This policy applies to all authorised users of departmental ICT facilities in:

- Agriculture, Fisheries and Forestry
- Environment and Heritage Protection
- Natural Resources and Mines
- Energy and Water Supply
- National Parks, Sport and Recreation, and Racing

which includes:

- permanent, temporary and casual employees
- contractors and consultants
- trainees and cadets
- work experience and industry placements
- volunteers
- any third party authorised to use departmental ICT facilities and devices.

3. Policy

The use of personally owned mobile devices (BYOD) within partner departments while accessing departmental systems and information is permitted subject to the following conditions:

- an application for the service must have the appropriate financial delegation approval (as there is an associated service charge) and comply with any other specific departmental criteria
- the user acknowledges the terms and conditions of use for their personally owned device while using the service (Appendix A) and signs the Mobile Device Access Form (Appendix B)
- the user in signing the terms and conditions of use (Appendix A), accepts that ITP has some level of control over their personal device in exchange for access to corporate resources (such as network and email services)
- only approved devices will be used in conjunction with the service

4. Principles

The BYOD service is provided to promote efficiencies in the workforce.

Information security and the protection of departmental assets is the overriding consideration when providing a BYOD service. The BYOD service is distinct from mobile devices supplied and maintained by ITP or Departments that are provided to users where there is a specific workplace requirement.

The BYOD service is provided as an optional service and convenience to the user and is subject to a legally binding agreement, the 'BYOD Agreement – Terms and Conditions of Service, Access and Use' (Appendix A) that each user must read, understand, and agree to abide with. When signing the Mobile Device Access Form, the user acknowledges these terms and conditions.

Users are to utilise the BYOD service with respect to the terms and conditions of their employment.

Users must abide by departmental email and Internet use policies, Information Security policies, relevant work, health and safety policies and the Code of Conduct for the Queensland Public Service when using ITP managed networks and services through the BYOD service.

When users are accessing departmental information through the BYOD service, they must manage personal information in accordance with Information Privacy Principles in the *Information Privacy Act 2009,* and acknowledge that documents stored or captured on a BYOD that have an official or work-related quality, may be subject to access applications made under the *Right to Information Act 2009.*

The BYOD service is provided for personal convenience consistent with Minister for Employment, Training and Industrial Relations Directive No. 5/05 August 2005 Hours and Overtime. (No claim for overtime is to be approved where a user elects to work solely for his or her own benefit or convenience.)

The BYOD service can be used as an additional communication option within a telecommuting arrangement (i.e. arrangements using the departmental telecommuting policy) or other flexible work arrangements organised with the user's manager/director.

Each department may vary charging policies for the BYOD Annual Service Fee from time to time and may pay the fee for users at their discretion.

Each department will determine where users are eligible for reimbursement of personal costs such as telecommunications network charges and device charges.

5. Authority

Criminal Code Act 1899
Financial Accountability Act 2009
Information Privacy Act 2009
Public Records Act 2002 (Qld)
Public Service Act 2008
Public Sector Ethics Act 1994
The Right to Information Act 2009
Minister for Employment, Training and Industrial Relations Directive No. 5/05 August 2005. Hours and Overtime.

6. Responsibilities

Directors-General of serviced departments are responsible for determining the selection criteria for user access to the service.

Chief Information Officer, Information and Technology Partners is responsible for:

- defining and implementing BYOD controls and measures
- seeking reimbursement from business areas for administration and licence expenses associated with the software required to secure and manage the device
- establishing and maintaining a list of devices suitable for the service
- establishing and maintaining a list of device software that is suitable and unsuitable for devices to utilise the service

Managers and **Directors** are responsible for:

- authorising the use of personal mobile devices for business purposes and if required by the department, on the basis of a suitable business case
- maintaining a suitable work-life balance for staff when using the BYOD service

Users (authorised users) of personally owned devices that are using the BYOD service are responsible for signing an agreement that includes but is not limited to:

- acknowledging and signing an agreement specifying the terms and conditions of use for their personally owned device while using the service
- providing a device with a suitably serviced internet connection and data plan at their own cost
- agreeing to allow ITP to load manageability software on their device while the service is being provided
- accepting that their personal device can be viewed, monitored and logged by ITP manageability software (limited only to deliver the service) and may be remotely reset (i.e. erasing all data and applications) if a security breach occurs
- understanding that they are solely responsible for backing up any personal content on their device
- agreeing to keep their device updated and operational
- acknowledging that their department or ITP will in no way be responsible for damaged, lost or stolen personal devices while the user is performing departmental business on that device

- removing any corporately required software or applications when exiting the BYOD service or when they leave their department

7. Forms

Appendix A - Bring Your Own Device (BYOD) Agreement – Terms and Conditions of Service, Access and Use
Appendix B - Mobile Device Access Form

8. Definitions and glossary of terms

Bring Your Own Device or **BYOD** is a business concept where a user provides their own mobile device to be connected to a corporate environment to be used for work purposes.
Mobile device or smartphone/tablet is a mobile phone/tablet built on a mobile operating system, with more advanced computing capability and connectivity than a mobile phone.
Security breach is where:

- the number of incorrect Personal Identification Number (PIN) code attempts is exceeded in the allotted time
- the device is reported lost/stolen or is determined not in the control of the authorised user.

9. Review

This policy will be reviewed within one year from the effective date of the policy.

10. Version history and approvals

Date	Version	Action	Description / comments
15 January 2013	1.0	Endorsed by ITP CIO	New policy
06 February 2013	1.1	Approval for DEWS	Approved by DEWS IISC on 06/02/2013
12 February 2013	1.2	Approvals for EHP and NPRSR	Approved for NPRSR on 21/12/2012 by Director-General, National Parks, Recreation, Sport and Racing and approved for EHP on 06/02/2013 by Director-General, Environment and Heritage Protection
30 April 2013	1.3	Approval for DNRM	Approved by DNRM IISC on 11/02/2013
13 June 2013	1.4	Approval for DAFF	Approved by DAFF IISC on 24/05/2013
28 June 2013	1.5	Minor edits	Amended template content to include endorsement and approvals in Section10 and to move Scope to Section 2. Included qualifier for need for a business case by the applicant employee – “where required by the department”.
11 July 2013	1.6	Minor edits	Amended the name of the “Mobile Device Access Request Form” to “Mobile Device Access Form”. Updated link in Appendix B to current version of Mobile Device Access Form
5 September 2013	1.7	Minor edits	Amended Section 5.2 (b) of Appendix A to clarify that a departmental email account cannot be synchronised with an external email account and amended relevant sections to increase from five (5) to ten (10) the permitted number of incorrect passcode entry attempts prior to locking and wiping of the device.
10 October 2013	1.8	Minor edit	Updated link in Appendix B to the new version of the Mobile Device Access form.

11. Keywords

BYOD; email; mobile device; mobile phone; smartphone; iPhone; iPad; android; tablet; iOS;

12. Licence

This publication has been compiled by Information and Technology Partners, Department of Agriculture, Fisheries and Forestry.

Appendix A: Bring Your Own Device (BYOD) Agreement – Terms and Conditions of Service, Access and Use

1. Your Acceptance of Our Terms and Conditions

1.1 In these Terms and Conditions "We", "Us" and "Our" refers to the relevant Queensland government department or agency offering You the Service as stipulated in Your Authorisation.

1.2 These Terms and Conditions constitute Our Agreement with You for Your Use of the Service.

1.3 Your Use of the Service constitutes:-

(a) Your acceptance of these Terms and Conditions as a legally binding Agreement; and

(b) Your acknowledgement that You have read, understood and agree to these Terms and Conditions.

1.4 We may change these Terms and Conditions and modify this Agreement from time to time. Your continued Use of the Service constitutes Your acceptance of any and all changes or modifications. The Terms and Conditions are made available to You for viewing on Our intranet service for each department.

1.5 These Terms and Conditions are intended to operate in conjunction with Your Employment Conditions.

1.6 To the extent of any conflict between these Terms and Conditions and Your Employment Conditions:-

(a) Where Your Employment Conditions are capable either expressly or impliedly, of being made subject to a contrary agreement, then these Terms and Conditions prevail to the extent of the conflict or inconsistency; and

(b) where Your Employment Conditions are not capable, either expressly or impliedly, of being made subject to a contrary agreement, then Your Employment Conditions prevail to the extent of the conflict or inconsistency.

2. Annexure

2.1 Definitions used in these Terms and Conditions are in **Annexure 1**.

2.2 Additional Terms and Conditions (Security, Credential and Technical Support) are in **Annexure 2**.

3. Application, Authorisation and Licence to Use

3.1 You must make an Application and obtain Our Authorisation before Using the Service.

3.2 If We accept Your Application, We will notify You by email to Your address nominated in Your Application.

3.3 You warrant that information provided to Us in the Application is true and correct in all material respects and You acknowledge that We rely on it for the purposes of providing Your Authorisation to Use the Service.

3.4 Your Application may be refused by Us in Our sole and absolute discretion, including where You have not completed an application process correctly, have been unwilling or unable to provide Us with information We require, or where You do not meet Our requirements and/or assessment criteria for Your Use of the Service.

3.5 By making an Application You authorise Us to communicate with Our Service representatives for the purpose of considering and processing Your Application in accordance with clause 14 (b) (i).

3.6 We may apply restrictions to Your Use of the Service, including where You have not met Our assessment criteria. We will advise You of the general nature of the reasons for these restrictions and, if applicable, how these affect Your Permitted Purpose and Use of the Service.

3.7 Upon and following Your Authorisation:

(a) You may decide at Your own discretion to Use or not Use the Service;

(b) We do not impose any obligation on You to Use the Service whatsoever; and

(c) if and when You decide to Use the Service, You do so each time subject to and in accordance with these Terms and Conditions.

4. Licence to Use the Service

4.1 Your Authorisation is Our non-transferable, non-sub-licensable, non-exclusive, revocable licence to You for Your Use of the Service and any Content (to the extent We own copyright or are otherwise entitled to grant You a third party copyright Content licence) for the time period stipulated in the Authorisation or otherwise until the Authorisation is revoked, suspended or terminated in accordance with these Terms and Conditions.

5. Permitted Purposes

5.1 Your Access and Use of the Services is provided by Us to You for the Permitted Purposes only in accordance with Your Authorisation and subject to these Terms and Conditions.

5.2 You must not:

(a) assign, transfer or sub-licence Our License to You for Your Use of the Service to any third party, without first obtaining Our prior written consent on terms and conditions that we may impose in our absolute and sole discretion; and

(b) synchronise Your departmental email to an external email account on Your Device.

6. Employment Conditions

6.1 You must abide by and comply with all of Your Employment Conditions (which includes the Code of Conduct) as they apply to Your Use of the Service for Your Permitted Purposes when Using the Service.

6.2 In particular You must:

(a) not Use the Service in any manner involving illegal, malicious, deceptive or misleading activity;

(b) comply with all of Our standards, policies, procedures, guidelines, Content requirements, codes for Your Use of the Services including where incorporated as part of Your Employment Conditions and our reasonable instructions concerning and in relation to Your Use of the Service;

(c) give Us all relevant information and cooperation that We may reasonably require in relation to Your Use of the Service; and

(d) advise Us of changes in Your User Information, Credentials, and Employment Conditions and Your Device details required or in relation to Your Use of the Service.

7. Termination of Authorisation or Employment

(a) Upon any material change to Your Employment Conditions, including any promotion, redeployment, secondment, termination, redundancy, suspension or change in duties we reserve the right :-

(i) to require You to make a further Application; and

(ii) to modify, alter and amend or revoke Your Authorisation depending on the circumstances as communicated between You and Us.

8. Revocation, Termination and Discontinuance

8.1 We may:-

(a) revoke or suspend Your Authorisation at any time by notice from Us to You at Our sole and absolute discretion and/or convenience;

(b) terminate this Agreement upon written notice to You with immediate effect; or

(c) refuse, disband or discontinue the Service at Our sole and absolute convenience either without notice or with notice to You with immediate effect.

8.2 Upon Your receipt of a revocation, termination or discontinuance notice:

(a) You will make no further Use of the Service in accordance with the revocation, termination and or suspension;

(b) within five (5) business days after revocation or termination, You will destroy or delete any copies of Service Software or Content as stipulated in Our notice to You; and

(c) You will certify to Us by Your email communication to Us that You have complied with the above requirements.

9. Audit

9.1 You agree to grant Us access to, or otherwise make available within fourteen (14) days of receiving notice from Us, such Content related to your access which is reasonably required by Us for Our legal, auditing, Employment compliance and management purposes, and in so far as they apply to Our provision of the Service to You and Your Use of the Service.

10. Your Device

(a) Our Service is available to You as an Authorised User for Your Device only, as identified in Your Authorisation.

(b) You must not modify Your Device from the standard configuration supplied by its supplier or manufacturer, as this will compromise or invalidate Your Use of the Service. In this regard, You acknowledge and agree that ITP may block Your Device from accessing the Service when it has a non-standard configuration.

(c) You as an Authorised User may register a new device (at no charge), including an upgraded or replacement device (for example after Your [original] Device is lost or stolen), which will then become Your Device for Your Permitted Purposes and Your Use of the Service.

11. Security

(a) You are responsible for maintaining the confidentiality of Your Credentials, and for restricting any unauthorised access to and Use of the Service obtained by means of Your Device or otherwise.

(b) You must not disclose or share Your Credentials to any other party unless that party has firstly been Authorised in writing by Us.

(c) In the event of a breach of security, including where the security of Your Credentials are compromised, or where You have reason to believe that that Your Credentials security has been compromised, or Your Device is lost or stolen, you must:-

(i) immediately contact Us and notify Us of the security incident and comply with the instructions and directions that We may give to You; and

(ii) deactivate or bar any Use of the Service, including by changing Your Credentials in accordance with Our instructions and directions.

(d) You must comply with any and all of Your Credentials (Password and Passcode) and Our Service Software requirements as notified by Us to You and as set out in Annexure 2.

(e) You acknowledge and agree that in accordance with the Terms and Conditions contained in Annexure 2 that You will be locked out of Service by Us and the Service Software for Your Device will remotely reset to Your Device's factory default after 10 unsuccessful Passcode attempts;

(f) Where any lockout or reset referred in above sub-clause (e) causes loss, injury or damage to You and/or Your Device including any loss/deletion of Your data and personal configurations We accept no responsibility and You release Us from any liability for such loss, injury or damage to You.

12. Costs and Fees for Use of the Service

(a) Depending on Our charging polices from time to time we may at our discretion pay the annual fee for Your access to and use of the BYOD Service (Annual Fee),

(b) Where we do not make the Annual Fee payment we will notify You in which case You are responsible for making such payment for Your Use of the Service.

(c) Apart from the Annual Fee payment as provided in above sub-clauses (a) and (b), You must bear Your own costs arising out of Your Use of the Service including where Use of the Service results in third party imposed charges, costs and fees, or Your Device and any costs in relation to applications purchased by You For Your Use of the Service, including any Use of the Service that results from third party, theft or fraudulent use of Your Device Credentials.

(d) Financial or in-kind reimbursement including any additional wages for time spent, banked time or flex arrangements in lieu, will be provided by Us for Your Use of the Service in accordance with your Employment Conditions as facilitated or agreed through your Employment supervisor.

13. Service and Content Availability and Integrity

(a) We are not obliged to support the Service Software for Your Use of Service in any way whether by providing advice, error-correction, modifications, updates, new releases, enhancements or otherwise.

(b) Your Use of the Service may be subject to unavailability, including emergencies, third party service failures, transmission, equipment or network problems or limitations, interference, signal strength, and maintenance and repair and control of speed of transmission of data including use of the Portal, and the Service Software to Use the Service.

(c) Delays or omissions in Your Using the Service may occur. Actual network speed will vary based on Your Device configuration, location, compression, network congestion and other factors.

(d) We are not responsible to You for any interruption or variation of Service or Content lost, not delivered or misdirected because of interruptions or performance issues with the Service, for whatever reason.

14. Personal and Confidential Information

(a) We collect and record User Information that You may generate by Your Use of The Service.

(b) You consent to Us accessing, collecting and using Your User Information solely for the following purposes:
(i) For use by Our authorised personnel for the purpose of considering and processing Your Application;
(ii) Our delivery of the Service including the Portal and Service Software management and Service security and administration and all technical, legal and Employment compliances and administration in relation to Us providing the Service; and
(iii) Where We may share information about You with other Queensland Government departments and agencies or other related organisations where it: - (A) is necessary to provide You with the Service or Your Use of the Service; or (B) is required or authorised by law; or (C) where a security threat has been made to the service or where it is considered likely that a security threat will be made to the service.

(c) When Using the Service You will only disclose Content that is confidential to those either expressly authorised to receive such confidential Content, or where consent has been obtained in writing from Your Employment supervisor or manager to disclose such Content to those who need to know for the Permitted Purposes.

(d) This Clause 14 does not apply to information that: - (i) has become public knowledge through no breach of an obligation of confidence by You; and (ii) is required to be disclosed pursuant to law provided that You give Us sufficient notice of such disclosure to allow Us a reasonable opportunity to object to and consider the taking of legal action to prevent such disclosure.

15. Third Party Content

(a) In Accessing and Using the Service there may be information, technology and software products and services of third party providers that are subject to separate additional terms and conditions ("**Third Party Information"**).

(b) You must abide by these third party terms and conditions when accessing and using Third Party Information while Accessing and Using the Service. To the extent of any inconsistency between these Terms and Conditions and the third party terms and conditions governing their intellectual property, the third party terms and conditions apply.

(c) We have the right, including as part of a suspension, revocation or termination decision under clause 8 of these Terms and Conditions to block or remove (in whole or in part) any Content communications and materials transmitted through Your Use of the Service that We believe in Our sole discretion may violate applicable law, this Agreement or a third party's rights, or that is otherwise inappropriate or unacceptable, including in response to lawful process, orders, warrants or subpoenas, or to protect Our rights, property and users.

16. Disclaimer

(a) We provide the Service as an optional service and convenience to You, and subject to these Terms and Conditions, You Use the Service at Your sole responsibility and risk.

(b) The Service, Content and Service Software is provided by Us to You on an "as is", "as available" basis without warranties of any kind.

(c) You are solely responsible for:-

(i) evaluating the quality, content, accuracy, adequacy, completeness, accessibility, suitability, safety, security, reliability, completeness, and usefulness of the Service and Content for Your Permitted Purposes;
(ii) for the installation of any and all updates for Your Device's operating system software applications as they become available and notified by Us for Your Use of the Service; security storage or back-up of Content, Your User Information and Your Device.

17. Limitation of Liability

(a) We exclude, to the maximum extent permitted by law any and all warranties, conditions, and representations, whether express, implied or statutory, that the Portal, Service, Your Use of The Service, Content and Service Software (**"Resources"**) will comply with any specifications, perform in any particular way, or be useful for any particular purpose or that the Resources are free from errors, defects, or (for Service Software) free from viruses or any other like or similar contamination.

(b) To the full extent permitted by applicable law, in no event will We be liable to You or any third party, on any legal basis (including without limitation, negligence) for any loss or damage whatsoever, including for special, incidental, indirect, consequential, punitive or exemplary damages arising out of or in connection with: (i) Your Use of the Service; (ii) Our providing the Resources; (iii) Your Device (including as a result of any default, reset, lockout or bar as a result of a security breach); or (iv) infringement of the intellectual property rights or moral rights of any person.

18. Indemnity

You agree to release, indemnify, defend and hold Us harmless from and against all third party claims, expenses, damages and costs (including legal costs) of any nature and howsoever arising made against Us (either directly or through You) for Your Use of the System and/or arising out of Your Device's factory default remote or loss/deletion of Your data and personal configurations under sub-clauses 11 (e) and (f) of these Terms and Conditions.

19. Governing Law

You agree that these Terms and Conditions and Your Agreement with Us shall be governed by and interpreted in accordance with the laws of the State of Queensland, Australia.

20. Survival

The following clauses survive termination of these Terms and Conditions: 12, 14, 15, 16, 17, 18, and this clause 20.

21. Severance

21.1 If any provision of these Terms and Conditions is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of these Terms and Conditions.

21.2 Without further action by Us or You, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

22. Entire Agreement

These Terms and Conditions constitute the entire agreement between You and Us governing Your Use of the Service.

23. Further Assurances

You agree to do, at Your own expense, everything reasonably necessary or requested by Us in order to give effect to the Terms and Conditions, including without limitation the execution and delivery of any required documentation.

24. Notices

24.1 All notices, consents, requests and other communications authorised or required to be given under this Agreement shall be given or confirmed in writing and either communicated by email or personally served on a party to whom it is given, mailed postage prepaid or sent by facsimile.

24.2 A party may modify contact details from time to time by giving written notice to the other of the modification.

24.3 A party must ensure that the other party has been notified of the current contact details for that party at all times.

Annexure 1 – Definitions

"Access" in relation to Using the Service means Your accessing the Service through Your Device as Authorised by Us and in accordance with Your Credentials;
"Agreement" means this legally binding agreement between You and Us formed upon Your acceptance of these Terms and Conditions in accordance with clause 1;
"Authorisation" means a written form notification in response to or as included on Your Application whereby We grant You a licence to Use the Service and Authorise Your Access for the Permitted Purpose; "**Authorised"** and "Authorised User" have corresponding meanings;
"Application" means Your written application using the template in Appendix B requesting Authorisation from Us to Use the Service;
"Annexure" means an annexure to this Agreement (Annexures 1, 2 and 3);
"BYOD" is an acronym for Bring You Own Device and describes the Service;
"Content" includes all information, reports, documents, data and datasets, databases, text, graphics, logos, software, design, photography, maps, video and other imaging, sound or other digital content, icons and illustrations contained within the Service, and/or submitted to or generated Using the Service;
"Credentials" means Your personal credentials, including, but not limited to Your user ID, Password, Passcode and digital certificate for Your Use of the Service;
"Device" means Your personally owned "mobile phone" device suitable for Your Using the Service and which is Authorised by Us to connect to the Service and which is the Device to be used by You as an Authorised user for the Permitted Purposes. Devices suitable for Use of the Service are listed on the ITP Intranet site at: http://intranet.daff.govnet.qld.gov.au/it/network/remote-access/mobile-mail
"Employment" means Your public service employment in accordance with Your employment role, conditions, description, responsibilities and contract with Us in pursuance of the *Public Service Act 2008* (Qld) and other applicable legislation and awards, and includes all applicable Queensland government information management, employment codes, policies and procedures in relation to conduct, human resources, intellectual property, privacy, information security, internet and email use in relation to the Service and Your Use of the Service. "**Employment Conditions"** has a corresponding meaning.
"ITP" means the Information and Technology Partners business group that provides ICT services to the Business and Corporate Partnership that comprises DAFF, DEWS, DNRM, DTESB, EHP and NPRSR;
"Our" "We", "Us" means the relevant Queensland Government department or agency offering You the Service as stipulated in Your Authorisation;
"Passcode" means the passcode that You allocate for Your Use of the Service as part of Your Authorisation in accordance with Annexure 2;
"Password" means the means the password that You allocate for Your Use of the Service as part of Your Authorisation in accordance with Annexure 2;
"Permitted Purpose" means Your Use of the Service for the purposes of Use of the Service as set out in Your Authorisation and made subject to the Terms and Conditions of this Agreement;
"Portal" means the MobileIron Self-Service Portal as used for the provision of the BYOD Service and includes technology applications in connection with Your Device geographical location, locking, remote reset and (device) applications.
"Service" means Our BYOD wireless communication network service as provided by Us and managed by ITP for Your Use of the Service for the Permitted Purposes in accordance with Your Authorisation and Credentials includes the Portal, Content and Service Software provided by Us to You now or in the future as generated by a Use of the Service;
"Service Software" means the manageability and other software for the Service that We may as provide from time to time for Your Use of the Service; Service Software includes the processes and any other ITP components that are used to store, retrieve manage and communicate the Content and for the Use of the Service;
"**Terms and Conditions**" means these terms and conditions as amended from time to time and made available through Our intranet services for each of our serviced departments;
"**Use of the Service**" means Your Accessing the Portal and Using the Service by Your Device and includes viewing, generating, submitting, and obtaining Content and undertaking transactions for the purposes and in accordance with this Agreement for the Permitted Purposes under Your Authorisation; "**Using the Service**" and "**User of the Service**" has corresponding meanings; and
"User Information" means any and all of Your personal information as defined under the *Information Privacy Act 2009* (Qld) generated or disclosed in Your Use of the Service and which may include information stored or communicated to or from Your Device as a result of:- (i) Your Use of the Service and Us providing the Service; (ii) Your Device's applications; (iii) geographic location of the Device (if not disabled); international mobile equipment identity (IMEI) number; (iv) general device type and specifications; (v) telecommunications provider; (vi) Your Device mobile telephone number (if supplied with the SIM card).

Annexure 2 – Additional Terms and Conditions - Security, Credential & Technical Support

1) When activating the Service, You must load on to Your Device the ITP Service Software (specific manageability software).

2) You must follow and comply with any and all instructions from Us or ITP that we may provide to You about loading the Service Software (specific manageability software) on Your Device.

3) You can elect to deactivate device specific location services on Your Device. Deactivating this service will not allow the ITP Service Desk to locate Your Device in the event that it is lost or stolen (We recommend that device specific location services remain activated).

4) ITP will automatically detect the types of applications and software loaded on the Device for security and compatibility reasons. This detection requires no human intervention (system generated) and records of this process are kept.

5) The ITP service to the Device will not be established if an incompatible application is loaded by You and the system will automatically notify You when this occurs. When the user removes the incompatible application the ITP service will be resumed.

6) ITP will remotely reset the device to its factory default settings (wiping all data and personal configurations) when the device's Passcode credential has been incorrectly entered ten (10) times successively.

Password

1) Your Password is used in combination with a user ID that forms an authentication process to obtain access to ITP services for the Device.

2) For security reasons, You will change Your password when requested to do so by Us and / or an authorised officer of ITP.

3) You understand that passwords will be at least 8 characters long and must contain at least 3 of the following 4 characteristics:

    a. lower case letter
    b. upper case letter
    c. number
    d. special character, limited to. !, #, $, &.

4) For example, #pA33w0rd! complies with this standard, but password01 does not.

5) Temporary passwords allocated to You will be changed at Your first login to the ITP services.

6) Failed login attempts may be monitored to determine if security is being compromised. Users will be locked out after 3 unsuccessful attempts.

Passcode

1) Your Passcode is Your Credential used to unlock Your Device for Your Use of the Service.

2) For security reasons, You will change Your Passcode when requested to do so by Us.

3) Your Passcode:

    a. must be at least 4 numbers in length
    b. must not be a permutation of a recognised user identification or easy to guess (e.g. date of birth, phone number, house number, 0000, 1234)

4) Failed login attempts using the Passcode may be monitored to determine if Device security is being compromised.

You will be locked out after ten (10) successive unsuccessful Passcode attempts and the Device will remotely reset to its factory default settings wiping all data and personal configurations.

Appendix B: Mobile Device Access Form

Available from:
http://intranet.daff.govnet.qld.gov.au/__data/assets/pdf_file/0018/12762/itp-mobile-device-access-form.pdf