USE OF SYSTEMS POLICY

1. PURPOSE

Energy Queensland Limited (**Energy Queensland**) and its related bodies corporate (referred to as members of the Energy Queensland Group) recognises that it and its employees, contractors, consultants, advisors, and agents (Users) rely on information and communications technologies (ICT).

Scope

This Use of Systems Policy (formally Agreement) outlines Users and EQL's obligations that apply to the use of Devices, computer equipment, licenced cloud-based Systems, network equipment, portable equipment, and other electronic Devices (collectively known as Systems) at Energy Queensland. This Agreement is in place to protect Users and Energy Queensland. Changes to this Agreement will only be included and implemented after consultation through the Industrial Relations Consultation Group (IRCG), consistent with the terms of the Enterprise Agreement

2. DEFINITIONS

In this Policy and any related documents:

Term	Definition
Authorised Use	Official use - required as part of your job function or relevant to your employment; this includes Reasonable Personal Use as defined in this document.
Data	Information that is held in, or accessed by, a Device or System in digital form that is in connection with Energy Queensland, its business activities, or Users.
Device	Any digital asset, computer equipment (such as a laptop or desktop), User Device (such as a mobile Device, phone, smart Device, tablet, or laptop), peripheral equipment (such as monitors and docks), network equipment, portable equipment, electronic Device or other Device or equipment used with or to access Data or Systems.
System	Any computer System, server, licenced cloud-based System, digital infrastructure, storage System, network Device or associated hardware.
User	Includes all employees, contractors, consultants, officers, partners, advisors, agents, and other Users who are authorised by Energy Queensland to access its Systems or Data.

3. SUPPORTING DOCUMENTS

The following documents support the implementation of this Policy:

Privileged Access Management Standard R199 – 691667

Employee Code of Conduct P004 – 691422

Information Security Incident Response Management - R062 - 690156

4. USE OF SYSTEMS IMPLEMENTATION

4.1. General Use and Ownership

4.1.1 Use of Devices and Systems

Users must utilize digital Devices and Systems for authorised business use. Personal use of Devices and Systems must notinterfere with work responsibilities. Users must respect intellectual property rights and comply with all applicable laws, regulations, and policies.

Only Energy Queensland approved, issued, or licenced Systems or Devices (including cloud-based services) must be used to interact with Energy Queensland Data or Systems while performing any job function. The use of privately owned or licenced Devices or Systems in this capacity is not permitted unless through a supported remote access method.

4.1.2 Ownership and Use of Devices

Devices are individually assigned to Users to perform their job function and are on loan from Energy Queensland. It is the User's responsibility to ensure Devices are appropriately maintained to agreed software versions and the Data and applications on them protected from Unauthorised Use.

4.1.3 Legal Status

Devices and access to Systems are provided for official use. Under Australian law Data in these Devices and associated Systems may be accessed under the Right to Information Act 2009 (Qld) and Information Privacy Act 2009 (Qld) or may be discoverable in the event of legal proceedings. This may involve both corporate and personal information if held on Energy Queensland owned Devices. EQL will work through the scope of any such requests with impacted personnel.

4.1.4 Device Management

All digital Devices must be maintained to ensure optimal performance and security. Users must notintentionally install software or applications which can compromise Devices and or Systems.

Physical damage or lost orstolen Devices must be reported as soon as reasonably practicable.

For Devices or Systems that have been stolen a User may be required to report the incident to the Police and complete a Police report.

4.1.5 Return of Devices

On cessation of employment orengagement by Energy Queensland, all Devices and other items and equipment owned by Energy Queensland must be returned as soon as reasonably practicable. Unless arrangements have been made for transfer of Device to the individual.

4.1.6 Employee Code of Conduct

All Users are required to comply with Energy Queensland's Employee Code of Conduct while using Devices and Systems for work purposes.

4.1.7 Installation of Security Updates and Patches

To ensure Devices and Systems are kept secure, and to ensure Energy Queensland complies with legislated security obligations, scheduled updates may be required or deployed by Energy Queensland to Devices and Systems. Users must notunreasonably

delay ordefer the installation of such updates and patches. Devices and Systems that are not kept up to date are considered vulnerable and may be remotely wiped.

4.1.8 Notification of Cyber Security Incidents

All Users have a responsibility to report known cyber security incidents involving Energy Queensland Devices, Systems, Data, or accounts as reasonably practicable. Early notification of cyber security incidents minimises their impact and consequences. Where appropriate, Energy Queensland will take steps in the event of an incident, to ensure employees are notified of any relevant information or actions needed as soon as reasonably practicable.

Users also have a responsibility to promptly report actual or potential theft ordisclosure of Energy Queensland-held Data including operational and personally identifiable information.

4.1.9 Participation in Cyber Security Awareness Program

All Users are expected to participate in security awareness and training activities provided by Energy Queensland and apply this security awareness and training in their everyday practices.

4.2. Reasonable Personal Use of Devices and Systems

Energy Queensland permits reasonable personal use of Devices and Systems.

Personal use must not:

- Interfere with business activities.
- Require hardware or software beyond the approved Energy Queensland configuration (including hardware connected wired or wirelessly).
- Require additional Device or System resources (such as compute, storage, or excessive Data allowances) beyond the approved Energy Queensland configuration.
- Knowingly introduce additional cyber security risk.

Personal use is not permitted on Energy Queensland Devices or Systems that are classified by Energy Queensland as not permitted for personal use.

Energy Queensland accepts no liability for any loss or damage suffered by Users because of any personal use of ourDevices or Systems.

Users shall not use your Energy Queensland email address when subscribing to online services or registering on websites that are principally for personal use.

4.3. Access to Systems

4.3.1 Accounts and Credentials

To access Energy Queensland Data, Devices and Systems, all Users will be provided with an assigned account consisting of a Username and passphrase. If required, you may also be issued with an authentication token. Some Devices and Systems may also permit the use of passcode, PIN, or biometric authentication as a complementary means of access.

Users must onlyuse their assigned account to access the Data, Devices, Systems, applications, and files to which they have been granted access. Users are responsible for all activity originating from their Username and accounts and must take reasonable steps to keep their account secure.

Users must not:

- Allow another person to use their account (other than through an email proxy arrangement).
- Deliberately attempt to access another person's account; or

- Attempt to access Data, Devices or Systems to which authorised access has not been specifically granted. The ability to inadvertently access, read, execute, or modify Data, Devices or Systems does not imply permission to do so.

4.3.2 Privileged accounts

Some Users may be given privileged access to critical Systems and highly confidential Data and/or the ability to modify orimpact Systems and the Data they contain. Obligations and requirements for this type of access is set outin the Privileged Access Management Standard R199 which must be complied with when granted privileged access.

4.3.3 Confidentiality of Credentials

Unless operating under an authorised exemption, the passwords, passphrases, passcodes, or PINs that are used to access Devices and Systems must:

- Be kept confidential.
- Meet Energy Queensland's complexity and length requirements.
- Not be shared with others including supervisors, co-workers, administrative or support staff.
- Not stored in an insecure manner (e.g., written down in an obvious place).
- Only be stored in password managers that are authorised by Energy Queensland; and
- Be changed when directed by Energy Queensland.

Users should immediately report any suspicion that your credentials have been compromised or used by others as a cyber security incident.

A User is permitted to share a passphrase, password, or PIN if:

- A System or Device that you access can only be configured with a shared password.
- You are receiving support from an authorised Energy Queensland support team member; and
- Under exceptional one-off circumstances where a General Manager orHigher-Level Manager has authorised a temporary exemption.

4.3.4 Remote Access to Data, Devices and Systems

Energy Queensland permits remote access to some Devices, Systems and Data, including as part ofworking from home arrangements. You may be provided access to Data, Devices or Systems from outside of Energy Queensland managed locations using a remote access solution. Remote access to Devices, Systems and Data is only permitted with the use of approved and Energy Queensland supported remote access mechanisms.

The use of non-approved remote access mechanisms is not permitted.

The use of public orfree Wi-Fi is not allowed due to cyber security risks other than in exceptional circumstances e.g. where there is no 4G or 5G network coverage. Remote access should be conducted only over known secure Wi-Fi connections or by using the in-built Data or hotspot functionality provided on Energy Queensland issued Devices.

4.3.5 Reporting of Unexpected Access to Devices or Systems

Unexpected access to a Device or System, e.g. access not required to perform a User's work function, should be reported as soon as practicable.

4.4. Access to Data

Energy Queensland Data may be accessed used or shared only to the extent authorised and that is necessary to perform a User's job function, in accordance with Energy Queensland's Conflict of Interest and Ringfencing policies.

When handling and using Energy Queensland Data, all Users must:

- consider the sensitivity of the Data - in particular operational, personally identifiable information and confidential information must be treated with additional care.
- Follow Energy Queensland guidance on classifying and handling information.
- Only store Data on Energy Queensland managed and approved services (such as SharePoint, OneDrive, Teams, ECM, Ariba, Xakia and corporate file shares).

Energy Queensland Data must notbe stored in other locations or services unless as part of an approved work instruction.

4.4.1 Reporting of Unexpected Access to Data

Any unexpected access to Data should be reported as soon as reasonably practicable to the Digital Service Desk and access to the Data ceased immediately.

4.5. Specific Requirements for Use of Email

4.5.1 Use of Official Email Account

All staff must ensure that all Energy Queensland official email is conducted only from an approved Energy Queensland email address. This ensures the proper management of records and the confidentiality of official business. The deliberate use of private email accounts to avoid record keeping, official review orscrutiny is prohibited.

Email rules must notbe set up to automatically forward official business to addresses outside of Energy Queensland, noting that payslips and other similar materials that would be considered personal in nature are excepted.

4.6. Cyber Security Safeguards and Device or System Management Tools

4.6.1 Filtering access to digital content

Energy Queensland may block orfilter access to selected external digital content including websites, emails, online services, or applications. Circumstances where this may occur include:

- Where the website, email, online service, or application has been classified as high-risk or contains or is likely to contain malicious or destructive code.
- Where access to the website, email, online service, or application places at risk the confidentiality orintegrity of Energy Queensland Data.
- Where Energy Queensland has been made aware of, or has reason to believe there exists, a security vulnerability orrisk in a website, online service, or application or in its operator, hosting provider orintegrator.

Due to the nature of these filters and safeguards, from time to time this may mean that:

- Legitimate email messages sent to Users may be delayed or blocked.
- Users may be unable to send an email message to another person; or
- Access to legitimate websites, online services, information, or applications may be blocked.

Energy Queensland has processes in place to recover blocked emails and to request the re-categorisation of websites, online services or applications should they be inadvertently blocked.

4.6.2 Removal of content orapplications from Systems

Energy Queensland may erase content from Energy Queensland Devices or Systems or perform a full or partial wipe of a Device or System without notice. This may include both business and personal Data. Circumstances when this may occur include:

- Where cyber security safeguards on the Device or System have been deliberately or accidentally bypassed or are otherwise considered ineffective.
- The Device or System or software on the Device or System has a high-risk security vulnerability.
- A Device or System is reported as lost orstolen or is suspected to be lost orstolen.
- A Device or System has been compromised or suspected of compromise in a cyber security incident, or contains compromised or suspected compromised content; and
- On detection of an excessive number of incorrect passcode, PIN or access attempts against an account, Device or System. Regular backup of personal items, such as photos, is encouraged.

4.6.3 Interception of messages and communications

Cyber security safeguards may intercept and analyse messages (including emails and messaging Systems) and communications (including contents of internet websites or files accessed from websites or cloud-based services) to detect the transmission of malicious code, internet link orclassified information, including over encrypted communications. Where issues are identified, procedures in accordance with the Energy Queensland Information Security Incident Response Management Procedure will be followed to address cyber related incidents.

Energy Queensland does not intercept the following communications:

- Secure messaging applications (such as iMessage and Snapchat); or
- Encrypted communications with websites categorised as health, nutrition, finance, accounting, Government or legal.

Data or information obtained from interception safeguards will not be relied on for the purpose of individual performance management and/or disciplinary action except where preliminary evidence confirms serious breach of policy omisconduct.

Where formal disciplinary action is proposed this will be in consultation with the relevant Union Officials, ensuring the confidentiality of discussion about anyindividuals is maintained. The parties will not unreasonably delay the consultation process. Where the matter is ofa serious nature, this clause does not prevent Energy Queensland from temporarily suspending an employee from duty while further investigation and consultation is undertaken. These actions are covered in more detail in Clause 14.6 of the Energy Queensland Union Collective Agreement –2024 and clause 14.2 of the Energy Queensland Retail Union Collective Agreement 2024.

4.7. Unacceptable Use

4.7.1 Installation of Unapproved Software on Devices or Systems

The installation of personally owned or otherwise unapproved software or applications that interact with Energy Queensland Data or Systems on any Energy Queensland Device or System is not permitted except on mobile Devices that are authorised for business and personal use, where applications may be downloaded for personal use from the Apple Store.

4.7.2 Use of Unapproved Cloud Services

Use of and storage of Energy Queensland Data in cloud computing services is only permitted using services that are officially authorised and appropriately licenced by Energy Queensland. For example, use of a sanctioned service e.g. Dropbox using corporate credentials would be permitted whereas storing EQL Data in the same service using personal credentials is not permitted.

4.7.3 Circumvention or Testing of Cyber Security Controls

Users must notreconfigure Energy Queensland Devices or Systems or deliberately seek to circumvent ortest security processes, policies, or controls unless you have formal approval. This includes resetting Devices or Systems to default orfactory settings, attempting to install alternate firmware, operating Systems, or jailbreaks, disabling or changing cyber security safeguards or Device or System management software, or performing any form of network, port orsecurity scanning or monitoring.

4.7.4 Use of Personal Credentials

Users must notconfigure a Device or System with a personal account (with the exception of a personal iCloud account which may be used for mobile Devices if preferred over an Energy Queensland issued account). All other Devices and Systems must only be configured or accessed with official Energy Queensland issued accounts. Personal applications may be installed on approved mobile Devices.

4.7.5 Use of Devices or Systems Outside of Australia

Devices or Systems may only be taken out of Australia with prior agreement. This is to ensure Energy Queensland remains compliant with legislated security obligations and can effectively manage Devices and Systems.

Depending on the destination country additional cyber security safeguards (including logging, monitoring, and restriction of usage) may be required to mitigate cyber security risks. In some circumstances where the cyber security risk is considered too high, requests to use Devices or Systems may be denied or alternate Devices or Systems may be provided specifically for use while travelling (and these may be disposed of once you return to Australia).

4.7.6 Removal or Substitution of SIM cards and e-SIMs

Where a Device or System has an Energy Queensland supplied SIM card or e-SIM Users are not to disable or remove the SIM card or e-SIM. Installation of a personal SIM card or e-SIM in a Device even if there is no Energy Queensland supplied SIM or e-SIM in the Device or System is not permitted.

5. ENFORCEMENT

Non-compliance with this Policy may result in disciplinary action, including termination of employment.

6. ACKNOWLEDGEMENT - USE OF SYSTEMS POLICY

To: Digital Office Service Desk

Email: servicedesk@energyq.com.au

I acknowledge that I have read the Use of Systems Policy and clearly understand my responsibilities in relation to the use of Energy Queensland's Systems and agree to comply with them.

(Please Print)

Full Name (User)	**Phone No**
Location	**Business Unit**
Position	
Signature (User)	**Date**
Supervisor Name	
Signature (Supervisor)	**Date**