Policy

POLICY TITLE:	**REMOTE ACCESS**
POLICY NUMBER:	**ICT-013**
CATEGORY:	**Organisational Directive**
CLASSIFICATION:	**Administrative**

<table>
<tr><th colspan="2">Approved by Council</th><th colspan="2">Meeting number and date</th></tr>
<tr><td colspan="2" rowspan="3">25 November 2014</td><td colspan="2">25 November 2014</td></tr>
<tr><th colspan="2">Resolution number</th></tr>
<tr><td colspan="2">3865</td></tr>
<tr><th colspan="2">Approved by CEO</th><td colspan="2">25 November 2014</td></tr>
<tr><th colspan="2">Effective date</th><th colspan="2">Review date</th></tr>
<tr><td colspan="2">30 October 2014</td><td colspan="2">30 October 2016</td></tr>
<tr><th colspan="4">Policy Author</th></tr>
<tr><td colspan="4">Chief Information Officer</td></tr>
<tr><th colspan="4">Endorsed by</th></tr>
<tr><td colspan="4">Director Corporate Governance and Financial Services</td></tr>
<tr><th colspan="4">Responsible Position</th></tr>
<tr><td colspan="4">Chief Information Officer</td></tr>
<tr><th>Current Incumbent</th><th colspan="2">Contact number</th><th>Email address</th></tr>
<tr><td>Robert Kane</td><td colspan="2">4846 3760</td><td>robert.kane@isaac.qld.gov.au</td></tr>
</table>

1. Purpose

Isaac Regional Council (IRC) issues mobile IT devices to some users to allow them to access IRC systems whilst away from their office. In addition, IRC has vendors and contractors who support and maintain IRC systems remotely.

Enhanced security of access from remote locations, compared to that of access from an IRC office is required to protect the security, integrity and confidentiality of IRC data from those who use public networks (the Internet) to gain illegal access to private data networks.

This policy defines the remote access to IRC networks and computer systems.

2. Scope

The policy covers remote access to all IRC networks and applications from offsite locations. The remote access could be via the Internet or via a dedicated link or phone connection.

3. Definitions

Term	Meaning
CIO	Chief Information Officer
IRC	Isaac Regional Council

4. Policy Statement

A remote access policy is essential in organisations where networks are geographically dispersed and extend into insecure network locations such as public networks or unmanaged home networks. It should cover all available methods to remotely access internal resources.

Users of IRC computer systems must comply with all relevant legislation, regulations and policies applicable to IRC.

4.1 General

Principles

General principles of remote access are:

- IRC network will be at all times protected by a firewall that controls the mix of traffic allowed into the IRC network. The mix will be based on operational needs and security concerns and will be determined by the Chief Information Officer (CIO).
- IRC reserves the right to block access through the firewall to any protocol, source address or destination address without notice to mitigate any perceived risk to network security or functionality
- Services available to remote users via direct Internet access will be limited to public services such as the IRC website and to password protected web services accessible

through staff portals (such as IRIS)

- Network services and software applications which require higher levels of security, such as administrative access to systems and access to file shares will only be accessible remotely via IT controlled technologies (currently Citrix and Virtual Private Networks but that may change). Such access is available to all employees, contractors and agents but authority for such access will be managed at individual system level and will come from business unit managers
- IRC reserves the right to monitor and inspect all remote access accounts issued to staff, contractors and agents to investigate suspected security breaches, inappropriate or illegal activity or unauthorised access
- Logs of remote access will be kept and monitored.
- Any unusual activity will be investigated

4.2 Requirements

- Users accessing any IRC password protected services remotely must ensure that the point of access provides an adequate level of security against private or confidential information being exposed to or intercepted by a third party. This is particularly relevant when using any form of wireless network
- Anyone using remote access to IRC computer services is bound by the same laws and policies that apply to internal access users. Examples include, but are not limited to the Password policy and the Email Use policy
- Personal equipment used to connect remotely to IRC networks must meet prevailing IRC requirements for virus protection
- Any requests for non-standard remote access must be approved by the IT Infrastructure team.

4.3 Authorities and Accountability

This policy applies to all authorised IRC users with an IRC owned, personally owned computer or workstation used to connect to the IRC network. This applies to remote access connections used to do work on behalf of IRC, including reading, sending email and viewing intranet web resources. Failure of authorised IRC users to comply with the above policies or users who have abused the use of remote access may have access removed and/or be subject to disciplinary action.

5. Communication Channels

The policy will be communicated throughout IRC via:

- An announcement on the IRIS intranet site
- Online Policy Library

6. References and Related Documents

- Password Policy
- Code of Conduct
- Cyber Crime Act 2001
- ICT Acceptable Use