Policy

POLICY TITLE:	**INFORMATION SECURITY**
POLICY NUMBER:	**CGFS-115**
CATEGORY:	**Council Policy**
CLASSIFICATION:	**Statutory**

<table>
<tr><th>Approved by Council</th><th colspan="2">Meeting number and date</th></tr>
<tr><td rowspan="3">22 July 2014</td><td colspan="2">22 July 2014</td></tr>
<tr><th colspan="2">Resolution number</th></tr>
<tr><td colspan="2">3713</td></tr>
<tr><th>Approved by CEO</th><td colspan="2">22 July 2014</td></tr>
<tr><th>Effective date</th><th colspan="2">Review date</th></tr>
<tr><td>7 July 2014</td><td colspan="2">7 July 2016</td></tr>
<tr><th colspan="3">Policy Author</th></tr>
<tr><td colspan="3"><b>Governance and Corporate Services</b></td></tr>
<tr><th colspan="3">Endorsed by</th></tr>
<tr><td colspan="3"><b>Director Corporate Governance and Legal Services</b></td></tr>
<tr><th colspan="3">Responsible Position</th></tr>
<tr><td colspan="3"><b>Senior Manager Governance and Corporate Services</b></td></tr>
<tr><th>Current Incumbent</th><th>Contact number</th><th>Email address</th></tr>
<tr><td><b>Aaron Johansson</b></td><td><b>4846 3549</b></td><td><b>aaron.johansson@isaac.qld.gov.au</b></td></tr>
</table>

1. Purpose

The Information Privacy Principle (IPP) 4 in the Information Privacy Act 2009 (Qld) (**IP Act**) relates to the security of personal information. It requires Isaac Regional Council (IRC) to ensure that they apply appropriate protections to the personal information they control. This means that even where documents are being held by another body or person, if the Council has the ability to exercise control over them, it must take the steps necessary to ensure they are protected.

This policy refers to Information Standard 18 – Information Security (IS18) under the IP Act. In some instances, compliance with such standards will be sufficient to satisfy IPP 4 (1)(a) and (2).

The aim is to implement a consistent approach to the implementation of information security to protect information assets, and any Information Communication and Technology assets which create, process, store, view or transmit information, against unauthorised use or accidental modification, loss or release.

2. Scope

This policy applies to all IRC employees and business units.

3. Definitions

Access: viewing information on a computer screen or reading a document through any medium

Confidentiality: restricting access to information to authorised persons, at authorised times, and in an authorised manner

Integrity: safeguarding the accuracy and completeness of information

Availability: ensuring that authorised users have access to information at authorised times

Information Asset: any intangible electronic information (separate from the media in which it resides) owned, controlled or hosted by IRC

Information System: item such as hardware, software, communications facilities and networks, used to store, process and transmit Information Assets owned, controlled, or hosted by IRC

Information Privacy Principle: IPP – Privacy principles under Information Privacy Act 2009

IP Act: Information Privacy Act 2009

IS18: Information Standard Information Security 18

Modification: Changing, removing or adding information

4. Policy

IRC must develop, document, implement, maintain and review appropriate security controls to protect the information IRC holds by:

- Establishing an appropriate information security policy, planning and delivering governance within the IRC in line with an information privacy standard, including adopting all specified frameworks, standards and reporting requirements
- Ensuring appropriate security controls are implemented as detailed by this policy

Adequate security safeguards

The security measures that IRC takes to protect documents containing personal information should be proportionate and appropriate to the possible risk of a security breach, and the level of harm that could result from a breach.

Some documents require more stringent security, based on the sensitivity or extent of the personal information including:

- Extensive amounts of personal information
- Information about vulnerable persons
- Sensitive information, such as racial and ethnic origin, political opinions, sexual orientation or criminal records
- Risk of identity theft or financial harm
- Risk of harm to a person’s life, safety, liberty, reputation or livelihood.

Need to know

The primary safeguard in protecting documents containing personal information is to limit access only to those who need to access it in order to do their jobs. IPP 10 and IPPs 1-3 should be considered when deciding who in IRC needs to have access to the information.

Steps should be taken to ensure that computer and physical files which contain personal information are not readily accessible to everyone in IRC. This is particularly relevant where IRC have implemented electronic document management systems, creating a central repository or index of all electronic files.

Controlling access involves more than deciding who should be able to access information. Other matters should consider, including:

- The necessity to limit the amount or type of information accessible to specific staff depending on their role
- What rights authorised staff should have to deal with the information i.e. ‘read-only’ access, or authorisation to change, add or delete information
- Permitted use of the information in almost all cases, staff should not access to held information for personal reasons
- Information accessibility to contractors - Considerations will include whether the organisation outsource functions or activities that involve information handling, or otherwise allow the contractor to access IRC’s premises or information technology systems

- What access, if any, is granted to external users' persons or bodies outside of IRC, and safeguards that are in place to protect the information Consideration include how many external users have access, to what extent- What protections or controls are in place to ensure the external users maintain the security of the information, and audit their access
- Who in IRC is authorised to grant access to information, and under what circumstances
- Who is authorised to disclose information to third parties and on what basis including clear criteria, protocols or policies for determining access and authority
- Authorised officers permitted to disclose the information and if there is a need to specify a list or class of persons or bodies who are authorised recipients or if there are persons or bodies to whom information should not be given because doing so could endanger the individual the information is about
- Which officers have full privileges for electronic information or are able to access all or most of the IRC document collections and minimising such officers to mitigate risk

Using audit logs

It is important that Council be able to determine if security has been breached and personal information has been accessed, used or disclosed contrary to the IP Act. Effective auditing will record who has accessed personal information, when and for what purpose, to both detect and deter misuse.

A visible audit process may also help to ensure that officers access personal information only for Council purposes, will also help to deter misuse. To be effective, audit logs or audit trails must be usable and used. Audits must be carried out and responsibility given to a person who can assess whether a potential breach has occurred.

Council needs to be able to interpret the audit log to determine what they need to know. The audit log should readily reveal who has accessed information, and when it is necessary to know what was done with the information, whether it was simply read, or whether it was copied, forwarded, modified, or deleted.

Securing physical storage

Another aspect of data security is physical security, concerned with controlling access to information repositories. These can be buildings, rooms, filing cabinets, compactus, laptop computers, USBs, briefcases or mobile phones. This involves assessing what physical barriers or practices can be used to prevent unauthorised access, misuse, modification, use or disclosure.

Buildings must be secured using a range of devices, such as locks on doors, swipe cards, security guards, access registers, or keypads. There may be multiple layers of authorised entry and access.

Where floor plans include lockable office and cubicle workstations, a degree of privacy and security for personal information is available. Where an office is open plan, and/or uses shared workstations and computers, consideration will need to be given to mitigating any privacy risks including:

- Adopting clean desk policies
- Providing separate conference rooms in which to meet with visitors or other Council staff
- Providing rooms to conduct sensitive interviews or telephone calls
- Lockable cabinets in shared workstations for each staff member
- Separate log-ins for shared computers, with secure workspaces for each staff member that cannot be accessed by other users who share the computer

Shared facilities

Consideration should be given to designing file rooms to maintain limited access to those persons with a need to know. Network and computer servers should be partitioned or restricted so that general access is limited.

Policies or work practices that provide guidance to staff, who are working in offices shared with other business units of IRC, will help to ensure the shared space does not lead to potential breaches of the IP Act.

Information on portable devices

Where personal information is stored on equipment such as computers or portable devices such as USB's, the information needs to be secured, particularly where they are taken outside of IRC.

Laptop computers

Upon leaving IRC premises, or where they are stored insecurely in those premises, a risk exists laptops to be lost or stolen. Safeguards should be used to ensure that if the equipment falls into the wrong hands, the information cannot be accessed. At the minimum, password protection and data encryption should be implemented, where possible.

IRC should ensure that staff are trained on proper use of IRC laptops, including what should and should not be stored on them. Policies will set out what an officer should do if they lose a laptop or suspect its integrity has been compromised.

Mobile phones

Personal information stored on IRC issued mobile phones such as contact details, text messages, video messages and photographs may be subject to the IP Act. If the device is a smartphone there is even greater potential for it to contain information subject to the IP Act. Where an officer is using a personal mobile phone for IRC business, IRC information stored on it may also be subject to the IP Act.

IRC should assess the extent to which technologies are used and security or privacy risks implications. Council must ensure that staff are aware of their privacy and security obligations when using Council issued devices, and are given guidance about the appropriate use of the mobile phone for work-related messaging. Password or PIN protection must be used to limit unauthorised access to the device and its contents.

Securing data during and after its transmission via facsimile

Facsimiles do not generate a paper document, being computers that send, receive and store data electronically. Increasingly, facsimile machines are being combined with scanning and copying functions, with increasing potential to store information. As such, IRC must apply similar protections to these multi-function machines (many of which have the capacity to email documents directly) as they do to computers. When transmitting documents, there is potential for the information to be disclosed to more people than the intended recipient. If the wrong number or email address is used, personal information may be disclosed contrary to the IP Act. If no record is kept of the numbers dialed or email addresses sent to, it may become impossible to determine to whom the information was accidentally disclosed.

Some steps to ensure security are:

- Isolating the fax machine in a secure area, ensuring only authorised persons can read faxes containing personal or otherwise confidential information
- Using cover sheets which indicate the total number of pages faxed, and informing the recipient that the remainder of a transmission contains personal information or is otherwise confidential
- Confirming the number before dialing, including a periodic check of pre-programmed numbers, to ensure they are accurate
- Phoning ahead to advise that a facsimile of a sensitive nature is coming
- Checking the confirmation report to confirm the accuracy of the destination number and the correct number of pages transmitted

Emails

Emails have significant amounts of personal information attached, and if sent outside of the IRC should not be considered to be secure. Information sent to an intended recipient can be intercepted or circulated to those with no authority or need to know it. Care should be taken to make sure that email addresses are accurate and up to date and unnecessary copying or forwarding eliminated.

IRC should enhance and maintain the security of emails and consider the following steps:

- Establishing what personal information is permitted to be sent via unencrypted email, and whether alternative means of transmission, is more appropriate based on the sensitivity of the personal information
- Determining when and what level of encryption is to be used, having regard to any prior need to establish suitable arrangements, by providing digital certificates
- Adopting an email disclaimer to warn all recipients that the contents of the email may contain personal information, and that privacy should be respected at all times. It should set out what steps should be taken if the email is received by someone other than the intended recipient, including notifying the sender and confirming whether the errant email should be deleted

Online information

When IRC collects or disseminates personal information over the internet, computer or coding errors can result in unauthorised access or disclosure on a world-wide scale.

Once personal information is placed on the internet, it may be difficult or impossible to retrieve it. Organisations such as Google, through its cache function, collect and store copies of websites. This information remains available on various sites, even if the owner of the website deletes the information from their own.

While there are methods by which this information can be removed, they can be complicated and cumbersome and, if an individual has copied and placed the information on a personal website, or stored it in their records, there may be no way for the IRC to have it removed.

If IRC is considering using the internet to collect or make available personal information, it must consider privacy and security at each stage before, during and after collection or dissemination. Council should consider ways to reduce the likelihood that search engines can seek out the information or archive storing it. Special coding may be used to repel search engine robots and spiders, so the website is excluded from internet search engines, and IRC must have plans in place to deal with any breaches that occur.

Document protection

IRC must ensure that officers understand their responsibilities and obligations under the IP Act by providing clear guidance about appropriate access, use and disclosure. They should provide copies of policies and procedures to officers and ensure they understand their obligations under the IP Act and the organisation's internal policies. Staff must be trained and relevant information should be included on log-in screens and in handbooks, policies and procedures.

Loss

Information can be including intentional or inadvertent destruction, and can be temporary or permanent, partial or total.

Unauthorised use, access, modification, disclosure or misuse

Unauthorised access may occur where a staff member uses their access privileges for personal reasons to:

- Satisfy their curiosity about any person
- Gain an advantage for themselves or any other person
- Access information they would otherwise have to buy
- Access the information for someone else.

Disclosing information means causing any other person to know it by opening it to view or revealing it. Unauthorised disclosures will include those disclosures that are not permitted under IPP 11 or, where it would be authorise under IPP 11, the officer in question was not authorised to make such a disclosure.

Access, modification or disclosure of personal information may be regarded as unauthorised where the person:

- Has no authority to access, modify or disclose the information, including where there is a legal restriction on access, modification or disclosure, where the person is not employed by IRC and has no authority to deal with the information, or where the person obtains the authority by fraud or deception.

- Exceeds their authority, for example, where the person goes beyond their limited authority to view more information than they are permitted to view, to make certain types of modifications they are not permitted to make, or to persons or bodies not authorised to
- Misuses their authority, by accessing information they are entitled to access, but for an ulterior purpose or motive, such as disclosing information for personal financial gain

Unauthorised disclosure and security breaches

Actions that breach IPP 11 that sets out when IRC may disclose information may also be a breach of IPP 4, but only where the breach occurred because of a failure to properly secure the information. IPP 11 focuses on the activities of IRC in proactively disclosing the information, while IPP 4 focuses on preventing unauthorised disclosure by IRC, and unauthorised access by people outside of the IRC.

Information may be inappropriately disclosed even where adequate protections have been put in place. Even where IRC takes steps to ensure that information is protected; security precautions may have been circumvented or ignored, including training implications dealing with personal information.

Careless, negligent or accidental disclosures may be considered a breach of both IPP 4 and IPP 11 where there were steps the IRC could have taken to better secure the information, through better training, records management or auditing practices.

Security breach notification

IPP 4(1) sets out the protections IRC has to place on safeguarding personal information. IPP 4(2) requires that those protections include security that individuals would reasonably expect the IRC to provide.

It may be necessary in the event of a disclosure (in breach of IPP 4) to notify an individual whose information was the subject of the breach.

Some basic factors for IRC to adopt when deciding whether to notify individuals that their privacy may have been breached include notifications, the steps IRC should go through in coming to a decision about whether notification is warranted in particular circumstances.

One of the objects of the IP Act is to provide for the fair handling of personal information. The objects of the Act must be kept in mind when applying the Act. When considering the requirement of IPP 4(2), IRC should notify affected individuals of data breaches involving their personal information.

Deciding whether to notify

When deciding whether or not a breach affects an individual Council must consider factors within the context of the personal information and the circumstances of the breach as follows:

- The potential for reasonably foreseeable harm to result from the breach for the person whose information is involved or otherwise affected, in particular its sensitivity, the amount of information, the extent of the unauthorised access, use or disclosure, the number of likely

recipients, the risk of further access, use or disclosure, especially in mass media or online, and any relationship between the recipient(s)
- The extent to which the person/s may already be aware of the breach of their information privacy
- Whether, notification is reasonably likely to alleviate or harm

Service providers

Under IPP 4(b), if IRC gives a document containing personal information to a person or body in connection with the provision of a service to Council, it must take all reasonable steps to prevent unauthorised use or disclosure of personal information including:

- Policy, planning and governance
- Asset management
- Human resources management
- Physical and environmental management
- Communications and operations management
- Access management
- System acquisition, development and management
- Incident management
- Business continuity management
- Compliance management

5. Mandatory principles

Principle 1 - Policy, planning and governance

IRC must recognise the importance of, and demonstrate a commitment to maintaining a robust information security environment. IRC at a minimum must:

- Develop an Information Security Policy
- Establish and document information security internal governance arrangements (including roles and responsibilities) to implement, maintain and control operational information security within IRC
- Establish and document information security and external governance arrangements to ensure that third party service level agreements and operational level agreements clearly articulate the level of security required, and are regularly monitored

Principle 2 - Asset management

IRC must implement procedures for the classification and protective control of information assets (regardless of format). IRC may wish to extend existing information asset and technology registers to incorporate security classification and control requirements. IRC at a minimum must ensure:

- All information assets are assigned appropriate classification and control
- All ICT assets that create, store, process or transmit security classified information are assigned ICT asset custodians

Principle 3 - Human resources management

IRC must minimise the risk of loss or misuse of information assets by ensuring that security controls are incorporated into human resource management, including the development of supporting policies and processes. At a minimum, IRC must:

- Implement induction and on-going training and security awareness program to ensure all employees are aware of and acknowledge the IRC’s information security policy, security responsibilities and associated security processes
- Document and assign security roles and responsibilities where employees have access to confidential information or perform specific security related roles, and ensure that security requirements are addressed in recruitment and selection and in job descriptions

Principle 4 - Physical and environmental management

The level of physical controls implemented must minimise or remove the risk of equipment or information being rendered inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation. At a minimum, IRC must ensure that policies and processes are implemented:

- To monitor and protect the use and/or maintenance of information assets and ICT assets away from premises
- For the secure disposal or reuse of ICT assets which are commensurate with the information asset’s security classification level

Principle 5 - Communications and operations management

Operational procedures and controls must be documented and implemented to ensure that all information and ICT assets are managed securely and consistently, in accordance with the level of required security. IRC must at a minimum ensure:

- The security of data during transportation over communication networks
- A network security policy is developed
- Controls are defined and implemented for the prevention, detection, removal and reporting of malicious code on all ICT assets
- Systems maintenance processes and procedures including operator and audit/ fault logs, information backup procedures and archiving must be implemented
- Operational control procedures are implemented to ensure that changes to information processing facilities or systems are appropriately approved and managed
- Methods for exchanging information within IRC, through online services, and/or with third parties are compliant with legislative requirements
- Processes are developed and implemented to review and test firewall rules and associated networks to ensure the expected level of network perimeter security is maintained

Principle 6 - Access management

Control mechanisms based on business requirements, assessed/accepted risks, information classification and legislative obligations must be in place for controlling access to all information assets and ICT assets. At a minimum, IRC must ensure that:

- Authentication requirements, including on-line transactions and services, are assessed
- Policies and/or procedures for user registration, authentication management, access rights and privileges are defined
- Control measures are implemented to detect and regularly log, monitor and review information systems

Principle 7 - System acquisition, development and maintenance

During system acquisition, development and maintenance, security controls must be established and the security classifications of the information contained for information systems, network infrastructure and applications. IRC must at a minimum ensure:

- Security requirements are addressed in the specifications, analysis and/or design phases and internal and/or external audit are consulted when implementing new or significant changes to financial or critical business information systems
- Processes (including data validity checks, audit trails and activity logging) are established in to ensure development and support processes do not compromise the security of applications, systems or infrastructure
- Processes are developed and implemented to manage software vulnerability risk for all IT security infrastructures

Principle 8 - Incident management

Effective management and response to information security incidents is critical in maintaining secure operations within IRC. IRC at a minimum must:

- Ensure information security management procedures are established to ensure appropriate responses in the event of information security incidents, breaches
- Ensure all information security incidents are reported and escalated through appropriate management channels
- Establish and maintain an information security incident and response register and record all incidents
- Ensure that security incidents caused by employees are investigated and where it is found that a deliberate information security violation or breach has occurred, that formal disciplinary processes are applied

Principle 9 - Business continuity management

A managed process including documented plans must be in place to enable information and ICT assets to be restored or recovered in the event of a disaster or major security failure. At a minimum, IRC must:

- Establish an information and ICT asset disaster recovery register to assess and classify systems to determine their criticality
- Establish plans and processes to assess the risk and impact of the loss of information and ICT assets in the event of a disaster or security failure
- Develop methods for reducing known risks to information and ICT assets
- Ensure business continuity and ICT asset disaster recovery plans are maintained and tested to ensure systems and information are available and consistent with service level requirements

Principle 10 - Compliance management

IRC must ensure compliance, and appropriate management of all legislative and reporting obligations relating to information security. IRC at a minimum must:

- Ensure that all reasonable steps are taken to monitor, review and audit information
- All information, processes and requirements including contracts with third parties are reviewed for legislative compliance on a regular basis and the review results reported

6. Communication Channels

The Information Security Policy will be communicated throughout the Council via:

- An announcement on the IRIS intranet
- Online policy Library

7. References and Related Documents

- Standards Australia (2001) Information Technology - Code of Practice for Information Security Management. AS/NZS ISO/IEC 17799:2001
- Information Privacy Act 2009
- Rights to Information Act 2009
- Queensland Local Government Information Security Processes

8. Acknowledgements

- Office of the Information Commission
- Queensland Government Information Security