Date received: **Allocated Case No:**

Subject Officer/s:

Is the allegation a CaPE Category 1, 2 or 3 matter? ***One / Two / Three (circle)***

Why? Please explain.

Does the allegation give rise to a suspicion of <u>Corrupt Conduct</u>?

Tick the applicable boxes below in order to make the assessment.

s.15 (2) Corrupt conduct might include:

(a) abuse of public office ☐
(b) bribery ☐
(c) extortion ☐
(d) secret commissions ☐
(e) fraud ☐
(f) stealing ☐
(g) forgery ☐
(h) perverting the course of justice ☐
(i) electoral donation offence ☐
(j) loss of revenue of the State ☐
(k) sedition ☐
(l) homicide, serious assault, or assault occasioning bodily harm or grievous bodily harm ☐
(m) obtaining a financial benefit from procuring prostitution or from unlawful prostitution engaged in by another person ☐
(n) Illegal drug trafficking ☐
(o) illegal gambling ☐

Mark any that apply and then consider your response to (a), (b), (c) and (d) below.

s.14 defines that conduct includes:

(a) neglect, failure and inaction; **AND**
(b) conspiracy to engage in conduct; **AND**
(c) attempt to engage in conduct.

NP_R

s.15 (1) Corrupt conduct - conduct of a person regardless of whether the person holds or held and appointment, that

(a) adversely affects (or could) directly or indirectly, the performance of functions or the exercise of powers of
(i) a unit of public administration (UPA); or
(ii) a person holding an appointment; ☐ **AND**

(b) results (or could) directly or indirectly, in the performance of functions or the exercise of powers mentioned in paragraph (a) in a way that:
(i) is not honest or is not impartial; or
(ii) involves a breach of trust ... either knowingly or recklessly; or
(iii) involves misuse of information or materials...; ☐ **AND**

(c) is engaged in for the purpose of providing a benefit to the person or another person or causing a detriment to another person; ☐ **AND**

(d) would if proved be:
(i) a criminal offence; or
(ii) a disciplinary breach providing reasonable grounds for terminating the person's services if they were a holder of an appointment. ☐

(a), (b) (c) and (d) must all be satisfied to amount to Corrupt Conduct.

Do we suspect <u>Corrupt Conduct</u>? **YES / NO** ***(circle)***

If yes, **report to CCC** via:

☐ N/A – Referred from CCC (Ref: MI- _____)
☐ S.38 referral (CCC Act); or
☐ S.40 referral (CCC Act); or

Additional comments

Assessed by:		**Date:**	
Signature:		**Position:**	Ethics Consultant, ESU
Reviewed by:	Neil BOYD	**Date:**	
Signature:		**Position:**	Executive Director, ESU

Complaint Assessment Form

Ethical Standards Unit

Date Received by ESU:	DD/MM/YYYY	**Allocated Case No:**	2014/2015-XXX
Subject Officer/s:	LAST NAME, First Name, Position title		
Workplace Details:	Business Unit, Division		
Complainant:	LAST NAME, First Name, Position title	Contact details	
Victim (if different):	LAST NAME, First Name, Position title	Contact details	Age:
Informant (if different):	LAST NAME, First Name, Position title	Contact details	
Whistle-blower (if different):	LAST NAME, First Name, Position title	Contact details	

1. Allegations

Précis of Allegations: [describe in a few sentences what is alleged to have happened]

For example:

The informant advised that the subject officer is known to "big note" himself by sharing information from IOMS with family and friends. The informant specifically referred to an email he has seen where the subject officer shared information about [name] a high profile prisoner with several other people including himself. The informant also remarked that the subject officer sat on the selection panel that awarded his sister-in-law a job.

Distil the allegation(s): [allegations need to be expressed such that if proven there is a case for remedial and / or disciplinary action]

For example:

*Allegation 1: It is alleged that [subject officer] **without authority** released confidential information from the IOMS database, in particular, information pertaining to [Prisoner First Name Last Name] to [name a party].*

*Allegation 2: It is alleged that [subject officer] **inappropriately** participated in the selection process in which [First Name Last Name], a relative by marriage, was a candidate.*

NP_R

2. Is the allegation serious enough, if proven, for disciplinary action to be considered by a decision maker per Section 187(1) of the Public Service Act 2008?

S187(1) Grounds for discipline [The most common grounds are bolded for easy reference]

(a) performed the employee's duties carelessly, incompetently or inefficiently; or
(b) been guilty of **misconduct**; [see definition below] or
(c) been absent from duty without approved leave and without reasonable excuse; or
(d) **contravened, without reasonable excuse, a direction given** to the employee as a public service employee by a responsible person; or
(e) used, without reasonable excuse, a substance to an extent that has adversely affected the competent performance of the employee's duties; or
(ea) contravened, without reasonable excuse, a requirement of the chief executive under section 179A(1) in relation to the employee's appointment, secondment or employment by, in response to the requirement—
  (i) failing to disclose a serious disciplinary action;
  (ii) giving false or misleading information; or
(f) contravened, without reasonable excuse—
  (i) a **provision of this Act**; or
  (ii) a standard of conduct applying to the employee under an approved **code of conduct** under the *Public Sector Ethics Act 1994*; or
  (ii) a standard of conduct, if any, applying to the employee under an approved standard of practice under the *Public Sector Ethics Act 1994*.

(4) In this section—
misconduct means—
  (a) inappropriate or improper conduct in an official capacity; or
  (b) inappropriate or improper conduct in a private capacity that reflects seriously and adversely on the public service.

Please note that the Code of conduct at 3.1 binds staff to adherence with whole of government directives, policies and standards and employing agency policies, organisational values and documents, so a breach of these is grounds for discipline as a breach of the Code of Conduct.

For example:

W-O-G IT Policy and Standards
JAG Workplace Policy
Operational Policies and Procedures specific to the environment.

Potential Breach(s) of Section 187(1) of the *Public Service Act 2008*? **YES / NO** ***(circle)***

Indicate likely breach(s) here:

For example:

If proven the conduct would be a breach of:

Section 1.5 of the Code - Demonstrate a high standard of workplace behaviour and personal conduct.
Section 1 of the JAG Workplace Policy – Showing respect for the dignity, rights and views of others.

3. Does the allegation have the characteristics of Corrupt Conduct under the Crime and Corruption Act 2001?

If referred from CCC as suspected corrupt conduct insert the CCC reference CC- _____).
[**Go to Section 5 – Public Interest Disclosure**].

Mark the applicable boxes below in order to make the assessment.

s.14 defines that conduct includes:

(a) neglect, failure and inaction; and
(b) conspiracy to engage in conduct; and
(c) attempt to engage in conduct.

s.15(1) Corrupt conduct - conduct of a person regardless of whether the person holds or held an appointment, that

(a) adversely affects (or could) directly or indirectly, the performance of functions or the exercise of powers of
  (i) a unit of public administration (UPA); or
  (ii) a person holding an appointment; ☐ **AND**

Please specify: [for example, through misuse of resources, information or powers, breach of privacy, execution of powers]

(b) results (or could) directly or indirectly, in the performance of functions or the exercise of powers mentioned in paragraph (a) in a way that:
  (i) is not honest or is not impartial; or
  (ii) involves a breach of trust ... either knowingly or recklessly; or
  (iii) involves misuse of information or materials; ☐ **AND**

Please specify: [or bold the relevant condition].

(c) is engaged in for the purpose of providing a benefit to the person or another person or causing a detriment to another person; ☐ **AND**

Please specify: [for example, to gain a benefit by avoiding some obligation imposed by the officer's duty – reading a magazine instead of performing 5 minute observations]

(d) would if proved be:
  (i) a criminal offence; or
  (ii) a disciplinary breach providing reasonable grounds for terminating the person's services if they were a holder of an appointment. ☐

Please specify the offence or disciplinary breach. [for example, accepted cash in exchange for confidential information related to a tender process.]

NB: (a), (b) (c) and (d) must all be satisfied to amount to Corrupt Conduct.

Would the conduct if proven amount to corrupt conduct? **YES / NO (circle)**

If you answered NO go to Section 4.

If you answered YES, continue below.

Alleged corrupt conduct is referrable to the Crime and Corruption Commission (CCC) where there are grounds for reasonable suspicion that it may have occurred. Is there a reasonable suspicion?

For suspicion to be 'reasonable', there needs to be more than bare or idle speculation (*George v Rockett* (1990) 170 CLR 104). In essence, there must be some evidence sufficient for a reasonable person to suspect corrupt conduct.

Mark the applicable boxes below in order to make the assessment.

Primary evidence:

- A complaint by the victim? ☐
- A complaint by a witness? ☐
- Clearly identified particulars (subject officer identity, date, time and location)? ☐
- Identified eyewitnesses or corroborating witness reports? ☐
- CCTV footage (usually available within 30 days)? ☐
- Medical evidence (for alleged excessive use of force/assault)? ☐
- Audit Report? ☐
- Other: (specify)_____

Secondary evidence:

- Hearsay evidence? ☐
- Anonymous letter, report or phone call etc.? ☐
- Other: (specify) _____ ☐

Consider carefully whether when taken together the available primary and secondary evidence raises a reasonable suspicion of corrupt conduct. Summarise your assessment below:

For example:

There are no particulars as to time, date and subject officer, and no incident or medical report related to the complainant in IOMS from which to identify the conduct complained of and from which to seek any CCTV footage. There are therefore no grounds to reasonably suspect corrupt conduct.

Do we reasonably suspect <u>Corrupt Conduct</u>? **YES / NO** ***(circle)***

If yes, select and mark the appropriate level as specified below

Level 1 – corrupt conduct by DG, executive or similar; abuse of office, extortion; secret commissions; administration of justice (pervert, fabricate, conspire etc); supply / traffic dangerous drugs; maladministration >$20K; use of force causing serious injury; sexual assault in custody; reprisal; imminent risk of abuse or neglect of detainee, officer with significant complaints history; media attention.

☐ Immediate referral to CCC via Form CO4

Level 2 - repeated behaviour of similar nature; fraud / misappropriation >$5K; a substantial injury; senior officer or supervisor failure to report corrupt conduct; potential systemic concerns

☐ Referral via s.40 schedule

Level 3 – Other matters not included above

☐ No referral – subject to audit.

If the conduct if proven would not amount to corrupt conduct, assess the complaint against the **Conduct and Performance Excellence (CaPE)** criteria below.

4. Is the allegation a Conduct and Performance Excellence *(CaPE) matter?*

Conduct	**Potential action**
Category One matters involve: • inappropriate interpersonal conduct with colleagues, clients or other stakeholders • inappropriate behaviour relating to minor management matters • performance requiring improvement. If you answered YES explain why:	**YES / NO** ESU advice **No role for ESU beyond advice**
Category Two matters involve: • ongoing or repeated inappropriate conduct with colleagues, clients and other stakeholders • minor misconduct: conduct / behaviour that is inconsistent with conduct standards expected of a public sector employee (such as the Code of Conduct), but that is not wilful or malicious • careless / negligent performance of duties (rather than unsatisfactory performance due to lack of skill). If you answered YES explain why *For example:* An officer displaying persistent low level nuisance conduct, inattention to rules and procedures, inappropriate language or engagement with colleagues or clients or similar.	**YES / NO** ESU advice OR
Category Three matters involve: • serious misconduct: conduct / behaviour that is inconsistent with conduct or professional standards / practices expected of a public sector employee (such as the Code of Conduct), and that is wilful, reckless or malicious • conduct that, if proven, will warrant the commencement of a discipline process, • conduct that, if proven, reasonably raises the possibility of termination of employment • conduct that is a breach of criminal law • serious neglect of performance of duties If you answered YES explain why. *For example:* *Being adversely affected by alcohol whilst on duty, and failing to report the absconding of a youth being supervised, are serious and reckless actions which if proven would attract a disciplinary sanction.*	**YES / NO** Investigation

5. Is the allegation a Public Interest Disclosure (PID)?

Mark the box if the condition is met.

Disclosure by any person:

- ☐ substantial and specific danger to a person with a **'disability'**
- ☐ substantial and specific danger to the **environment**
- ☐ **Reprisal** taken against anybody as a result of a PID

Disclosure by Public Officer:

- ☐ **Corrupt Conduct**
- ☐ **Maladministration**
- ☐ substantial **misuse of public resources**
- ☐ substantial and specific danger to **public health or safety**
- ☐ substantial and specific danger to **environment**

Is this a Public Interest Disclosure? **YES / NO (circle)**

If yes, conduct an immediate **risk assessment** (see PID Risk Assessment procedure)

PID Risk Assessment Outcome (Mark any that apply):
(Consult HR&G)

- ☐ Additional security
- ☐ Discloser declined support / protection
- ☐ Monitoring / management of staff who may engage in reprisal
- ☐ Protection of identity or existence of discloser
- ☐ Provision of tailored support for discloser
- ☐ Suspension of staff who may engage in reprisal
- ☐ Transfer of discloser
- ☐ Transfer of staff who may engage in reprisal
- ☐ Other (specify)
- ☐ Specific support provided? (comment):

Has the PID Register been updated? **YES / NO / Not applicable (circle)**

---

6. Matter to be handled by:

☐ Ethical Standards Unit ☐ Management action ☐ HR&G (staff dispute)

☐ Corrective Services Investigation Unit (CSIU) ☐ Employee Relations

7. Other referrals

- ☐ Queensland Police Service (for criminal matters)
- ☐ Internal Audit (material loss)
- ☐ HR&G for medical issue requiring rehabilitation liaison
- ☐ Ombudsman (PID database)
- ☐ Management action – immediate systemic issue
- ☐ Crown Law – legal opinion required
- ☐ Other (specify)

8. Recommended action (ESU Complaint Management) Mark any that apply.

- ☐ Secure documents
- ☐ Preliminary enquiries
- ☐ Return to Division for internal investigation
- ☐ ESU investigation
- ☐ External investigation
- ☐ Other (specify)

Further specific enquiries need to be undertaken in the form of:

For example: securing CCTV and officer incident reports, medical reports etc

9. Additional comments

Assessed by:		**Date:**	
Signature:		**Position:**	Ethics Consultant, ESU
Reviewed by:	Neil BOYD	**Date:**	
Signature:		**Position:**	Executive Director, ESU

ATTACHMENT 1

ATTACHMENT 2

Purpose:

The purpose of this policy is to ensure appropriate access management to information and associated information systems within the Department of Community Safety (DCS). This includes access requirements associated with DCS networks, applications, information systems, Internet, departmental email and personal usage of these resources.

Rationale:

To minimise information security risks in the department. To ensure intellectual property rights of the State are protected and that the department's information assets have the appropriate protection and controls from unauthorised access or accidental modification, loss or release. All departmental employees, contractors, volunteers and third party users are responsible for the security and protection of information assets over which they have control.

Application:

This policy applies to all employees, contractors, volunteers and third party users, who must be made aware of the department's responsibilities and commitments in this area and the part they can play in meeting these responsibilities.

Implementation:

This policy will be communicated on an ongoing basis and be accessible to all employees.

Policy Approval:

This policy, version 1.0 was endorsed by the Communication and Information Committee on 18/02/2010. This policy, version 1.0 was approved by the Director-General on 13/05/2010. This policy, version 2.0 was approved by the Assistant Director-General, Corporate Support Division on 20/03/2012.

This policy, version 2 1 was approved by the Deputy Director-General, Corporate Service on 13 November 2012.

Policy Review:

This policy is reviewed annually. The next scheduled review is November 2013.
This policy will also be reviewed and evaluated in line with changes to business and information security risks to reflect the current agency risk profile.

Table of Contents:

Policy:

The department provides a wide range of information services to the public, staff, partners and other jurisdictions of Government. The department has an obligation and responsibility to provide a duty of care and protection of clients, to maintain client confidentiality, and to establish and maintain the security and integrity of information and associated information systems.

Access control mechanisms consistent with business requirements and assessed/accepted risks must be in place for controlling access to all information, information systems, networks (including remote access), infrastructure and applications. Access controls must be consistent with the department's business requirements and information classification levels as well as legal and legislative obligations. Information and information systems are to be used for the following purposes:

- Conducting official departmental business;
- Deployment under declared incident/emergency situations;
- Education and self-development, as agreed with management;
- Commercial benefit of the State of Queensland; and
- Limited personal use.

Appropriate access controls assist to protect the department's information assets. The "defence in depth" principle should be followed based on a risk management process, and where appropriate using multiple "layers of access controls" to protect critical information.

The department must ensure all information and associated information systems are issued a classification level to determine the level of access controls required.

Formal procedures must control how access is granted to information systems and how such access is modified and / or removed, so as to mitigate unauthorised access to information assets.

Access must be in accordance with legislative and regulatory requirements to either provide, or to deny, access to information.

Authentication:

Authentication will be governed by the *Queensland Government Authentication Framework*. At a minimum, passwords will be used to authenticate users to the DCS Information and Communication Technology (ICT) computer networks and associated information systems. Stronger authentication may be instituted for high risk or business critical systems or applications as deemed necessary.

User Access:

Information and Communications Systems (ICS) Operations is responsible for electronic account management within the department's information systems to ensure authorised access to information and applications. Security processes are required to be established and resourced to facilitate the process of withdrawing access rights and credentials as necessary.

For purposes of accountability and traceability, all departmental employees, contractors and third party users must be issued with unique access credentials that provide them with the means to access relevant information or information systems for which they have been authorised. Generic accounts, including generic email accounts, are not to be created and utilised. For specific business and operational needs, generic accounts may be exempted from this requirement in writing by the Executive Director, ICS or delegate.

Authorised parties must sign a statement acknowledging the access rights granted and their requirements to appropriately manage the access credentials. This is in addition to the authorised parties signing a statement that they have read and understood the applicable departmental security policies.

All requests for a user or service account to be created, modified or removed, must be approved either in writing and sent to the ICS Service Centre or via the ICSystems Customer Portal by the person's direct Manager or Supervisor.

To mitigate unauthorised access, user and service accounts will be restricted to only the required necessary privileges to perform their duties.

Use of the department's information and information systems, including, but not limited to, internet, email and messaging services usage is monitored. As such, all personnel accessing the information and information systems shall have no expectation of privacy as it pertains to the use of departmental information or information systems.

Internet:

All requests for access to the internet are to be made through a user's manager to assist departmental users in the performance of their assigned work duties.

All software used to access the internet must be part of the department's standard software suite or approved by the Information Security Unit.

All information systems and devices used to access the Internet shall be configured by ICS Operations to use the department's Internet Gateway and pass through any access control and monitoring devices. Access to the internet without passing through the access control or monitoring devices is prohibited except where the configuration has been modified by authorised staff to support emergency incidents/situations, or a specific exemption has been granted for operational purposes and approved by the Executive Director, ICS or delegate.

Access to the internet via the department's network connection from an employee's home-based computer (whether the computer is owned by the department or not) must adhere to all of the same policies that apply to use from within departmental facilities, including not allowing family members or other non-employees to use departmental information systems.

Email:

All requests for access to electronic messaging services are to be made through a user's manager to assist departmental users in the performance of their assigned work duties.

Any electronic messages created, transmitted or stored on information systems owned, leased, administered, or otherwise under the custody and control of the department are not private and are owned by the department. As such this data may be accessed by the department at any time.

Upon approval by a member of the DCS Executive Leadership Team, 'bring your own' ICT mobile devices as defined in the *DCS 'Bring Your Own' ICT Mobile Device Policy* may be used for specific business and operational needs. Employees that have not received approval from a member of the DCS Executive Leadership Team must only use departmentally-issued and managed mobile communication devices to connect to the department's electronic messaging systems to send, forward, receive or store departmental communications or information.

Unless authorised in writing by the Executive Director, ICS or delegate or utilising 'bring your own' ICT mobile devices, externally-hosted web-based email solutions such as but not limited to, hotmail or gmail are not to be accessed via the department's networks or Internet communication devices.

All classified departmental material transmitted over non-departmental and/or external networks must be encrypted.

All users must use appropriate email etiquette, professionalism and language in compliance with the *Code of Conduct for the Queensland Public Service* and information security policies and procedures.

Personal Use:

Limited personal use of the department's information resources, including Internet access, email and messaging services, is subject to, but is not limited to, the following restrictions:

- Use is not to result in direct costs to the department. The department reserves the right to require reimbursement of costs for excessive personal use.
- Utilising the department's services for personal monetary gain or for commercial purposes that are not directly related to the department is not permitted.
- Personal use must be professional, legal and consistent with the *Code of Conduct for the Queensland Public Service*, information security policies and procedures.
- Personal use is not to interfere with the normal performance of an employee's duties.
- Personal use is not to impact the business in any way, such as excessive utilisation of network resources, therefore causing a negative impact on the business use of the internet connection or other information systems.
- Use of information systems is restricted to departmentally-approved users only. It does not extend to family members or other acquaintances.
- Any personal files and documents created, accessed, sent and/or received via the department's information systems are subject to open records requests and may be accessed in accordance with the department's Information Security Policies, the *Information Privacy Act 2009* and the *Right to Information Act 2009*.
- The employee's personal use access rights may be revoked at any time at the discretion of the employee's manager should use be deemed to be excessive or interfering with the employee's performance of their duties.

Unacceptable Use of Information Resources:

What constitutes unacceptable use is ultimately a matter of fact, taking into account the *Code of Conduct for the Queensland Public Service* and departmental information security policies and procedures. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

Internet, Network and System Activities

- Unauthorised downloading, storage, installation, copying, sharing and/or use of copyrighted material, of any format, to include, but not limited to computer software, documents, images, video, movies and music.
- Posting, sending, accessing or attempting to access pornographic or sexually explicit/oriented material, hate-based material, computer/network hacking or cracking material.
- Use of non-standard software, to include but not limited to, shareware or freeware software unless it is on the department's standard software list, and if not, is authorised for use in writing by the Executive Director, ICS or delegate.

- Intentional writing, copying, executing, or attempting to introduce any malicious computer code or program (e.g. virus, worm, Trojan horse, etc.) designed to alter, damage or delete information and/or otherwise hinder the performance of or access to the information or information systems of the department or any external organisation.
- Attempts for unauthorised access or modifications to information or information systems, whether it belongs to the department or an external organisation.
- Intercepting, eavesdropping, recording, reading or altering communications unless authorised in writing by the Executive Director, ICS or delegate.
- Performing activities intended to circumvent the security or access controls of the department's information systems or of any external network, unless required to perform as part of authorised departmental duties or authorised in writing by the Executive Director, ICS or delegate.

Email and Communications Activities

- Any form of harassment via messaging, voice or paging services, whether through inappropriate language or images, frequency, or size of messages impacting the department's reputation or any person or external organisation.
- Unauthorised use, forging or modification, of messaging header information.
- Creating or forwarding "chain letters", or "pyramid" schemes of any type.
- Disseminating information via messaging services such as email and Internet forums without the appropriate management authorisation that may result in false representation of the department, personal opinions, disrupt business operations in any form or reveal sensitive personal or agency information.
- Performing impersonation activities without the appropriate authorisation.
- Sending unsolicited messages for the purpose of advertising, promoting personal business, lobbying and campaigning activities. This does not include activities associated with approved union activity or workplace issues in accordance with departmental and Government policy.

Network Access:

ICS is responsible for the development and implementation of processes and procedures concerning the use of networks and networked services. These will include:

- The networks and network services which are allowed to be accessed;
- Authorisation procedures for determining who is to be authorised to access which networks and networked services;
- Management controls and procedures to protect access to network connections and networked services.

Operating System Access:

- Policies and procedures must be defined, documented and implemented for the management of operating systems security, including user registration, authentication management, access rights and privileges to systems or application utilities.
- Access to agency information systems must be consistent with the department's Managed Operating Environment (MOE) and administrative privileges and will be consistent with the system securing configuration standards developed by the Information Security Unit.
- To prevent unauthorised system access, security controls at the operating system level must be used to restrict and protect access to information resources.

Application and Information Access:

- All systems, where possible, shall display as part of their logon prompt a logon banner advising that access to the system is restricted to authorised users only and that unauthorised access may be monitored and where appropriate will be disciplined to the highest extent possible under the law.
- Controls must be used to restrict and protect access within application systems. Access to software and information should be limited to authorised users.
- All applications and information systems will be consistent with the system securing configuration standards developed by the Information Security Unit.
- Security controls are to be implemented to restrict access within application systems.

Mobile Computing and Telework Access:

When using mobile computing facilities, e.g. notebooks, palmtops, laptops and mobile phones, special care is to be taken to ensure that business information is not compromised, especially when using these devices in public places, meeting rooms and other unprotected areas. As such, the use of security controls such as security cables or encryption must be considered.

The department must ensure all information and associated information systems are issued a classification level to determine the level of access controls required.

Departmental staff requiring access to information systems from outside of authorised departmental facilities or from locations that are not supported by the department's network, are to utilise the department's approved remote access facilities, following the requirements below:

- Remote access is restricted to authorised personnel only;
- All remote access to the department's network will be through the department's prescribed remote access gateway;
- Simultaneous connections to public networks, such as the Internet, while connected to the department's remote access network are strictly prohibited, except where the other network is used as a transport for a remote access connection;
- All remote access to the department's network over the Internet will be encrypted using the prescribed virtual private networking solution; and
- Appropriate technical security safeguards are to be deployed onto remote access devices and validated by the remote access gateway before the remote device is allowed to connect to the department's network.

Where wireless solutions are utilised, security controls should be implemented to ensure at least the equivalent level of security as the department's wired infrastructure.

Consequences of Non-Compliance:

Non-compliance with this policy, depending on the severity and nature of the non-compliance, may result in the department taking action in accordance with the *Code of Conduct for the Queensland Public Service.*

Roles and Responsibilities:

All departmental managers are responsible for:

- Where the delegated authority exists, authorising access to departmental information and information systems for users they manage;
- Communicating access changes of an employee's duties to the ICS Service Centre.; and
- Ensuring all employees under their management, including any contractors or third party users, are made aware of their responsibilities as users of DCS ICT services with regard to the requirements of the policy.

ICS Operations is responsible for:

- Centralised account management and administration of departmental electronic information systems;
- Managing access to the department's information systems in accordance with established access control rules;
- Implementing and managing perimeter access controls via the Internet Gateway devices; and
- Ensuring access controls throughout the department are implemented appropriately.

Information Management is responsible for:

- Development and maintenance of departmental policy, procedures and guidelines regarding access management;
- In consultation with ICS Operations, instigating an implementation strategy and associated processes to ensure compliance with information security policies and procedures and address deficient information security;
- Providing security advice and education strategy to ICS and divisional stakeholders by instigating a formal Information Security Awareness Program;
- Performing departmental information security compliance checks;
- Creating monthly information security reports for the Executive Director, ICS;
- Maintaining the department's Information Security Risk Register; and
- Working with project teams to oversee compliance to the departmental Information Security Policy Framework and the Queensland Government Information Standard 18: Information Security (IS18).

The Executive Director, ICS or delegate is responsible for:

- Authorising information systems support personnel to manage, administer and monitor the use of information and information systems within the department; and
- Approving any connection to the internet or other external network that is not through the authorised Internet Gateway.

All departmental employees, contractors, volunteers and third party users are responsible for:

- Reporting any weaknesses, including suspected breaches or incidents, in departmental information or information systems to their manager and / or the ICS Service Centre;
- Adhering to the requirements of this policy;
- Being cognisant of and compliant to the *Code of Conduct for the Queensland Public Service*, *Information Privacy Act 2009*, *Right to Information Act 2009* and DCS information security policies and procedures;
- Indicating their acceptance and understanding of any authorised use messages / legal notifications displayed as part of logon banners to an information system, network device or any other DCS ICT infrastructure. Successfully logging into a system which displays a legal notification indicates the user has read, understood and accepts the intent of the legal notification and understands and agrees to adhere to DCS Information Security Policies and Procedures;
- Only attempting to access information systems that they have been authorised to access, and only accessing those systems when it is related to their work related duties;
- Not connecting non-approved, externally provided and personal computing devices, such as employee-owned computers, personal digital assistants (PDAs), USB storage devices and other external devices locally, whether via physical or wireless means, to the department's networks unless authorised consistent with the DCS 'Bring Your Own' ICT Mobile Device Policy;
- Mobile phones connecting to the department's wireless network must utilise the department's existing wireless security device management solution. All departmentally-approved computing devices, whether connected to the department's network or standalone, must use the department's approved controls, unless deemed unfeasible or operationally inappropriate, based on a formal risk assessment;
- Only using departmentally-approved USB storage devices when connecting USB storage media to the department's computer networks and information systems. Departmentally-approved controls for USB storage devices, such as encryption and authentication must be utilised to mitigate the risk of electronic information being accessed if the device is lost or stolen. USB storage devices are not to be utilised as a standalone storage facility for departmental information. Departmentally-approved network storage and backup facilities must be utilised, unless authorised in writing by the Executive Director, ICS or delegate;
- Only purchasing and using USB storage devices as per the *DCS approved hardware website*, approved through a user's manager and procured via ICT Purchasing or a retail store. Only USB storage devices listed on the departmental *Approved USB Storage Device List* should be purchased, unless authorised in writing by the Executive Director, ICS or delegate; and
- Not using the department's information and information systems including, but not limited to internet and email, for the purposes of promoting or maintaining a personal or private business or for personal gain.

Superseded Policies:

- 15.2 - Security of DES Information & Communication Technology – Policy, v1.0
- 15.2.4 – DES Firewalls Practice Statement, v1.0
- 15.2.5 – Authorised Use of DES ICT Practice Statement, v1.0
- 15.2.6 – Remote Access Policy, v1.2
- Queensland Corrective Services Policy – Information Technology Device Usage - 23 July 2008
- Queensland Corrective Services Policy – Information Security - 24 July 2008

Links to Relevant Legislation, Policy and Guidelines:

Legislative Authority

- *Queensland Government Legislation,* to include:
  - *Criminal Code Act 1899* (QLD)
  - *Public Sector Ethics Act 1994* (QLD)
  - *Public Service Act 2008* (QLD)
  - *Electronic Transactions Act 2001* (QLD)
  - *Crime and Misconduct Act 2001* (QLD)
  - *Public Records Act 2002* (QLD)
  - *Right to Information Act 2009 (QLD)*
  - *Ambulance Service Act 1991 (QLD)*
  - *Fire and Rescue Service Act 1990 (QLD)*
  - *Corrective Services Act 2006 (QLD)*
  - Information Privacy Act 2009 (QLD)
  - *Financial Accountability Act 2009*
  - *Disaster Management Act 2003 (QLD)*
- *Commonwealth Government Legislation*, to include:
  - *Telecommunications Act 1997* (Commonwealth)
  - *Telecommunications (Interception) Act 1997* (Commonwealth)
  - *Cybercrime Act 2001* (Commonwealth)

Related Legislation

- *Financial and Performance Management Standard 2009* (QLD)
- *Queensland Government Information Standards*, to include:
  - *Information Standard 18 - Information Security* (QLD)
  - *Information Standard 19 - ICT Resource Maintenance & Disposal* (QLD)
  - *Information Standard 26 - Internet* (QLD)
  - *Information Standard 31 - Retention & Disposal of Public Records* (QLD)
  - *Information Standard 34 - Metadata*
  - *Information Standard 38 - Use of ICT Facilities and Devices* (QLD)
  - *Information Standard 40 - Recordkeeping* (QLD)
- Queensland Government Intellectual Property Guidelines
- *Australian Standards*, to include:
  - *HB:221:2004 Business Continuity Management*
  - *AS/NZS 4360: 2004 – Risk Management*
- *Queensland Government Information Security Policy Framework - Queensland Government Chief Information Office, Queensland Government Enterprise Architecture.*

The Queensland Government Information Standards do not override State and Federal legislation and regulations.

Related Government Guidelines

- *The Australian Government's Protective Security Manual* (Commonwealth)
- *Australian Government Information Security Manual* (Commonwealth)

Related Departmental Policy and Other Documents

- *Code of Conduct for the Queensland Public Service*
- Intellectual Property Policy

For Assistance Contact:

Business Unit	Phone Number & Email
Information Security Architect, Enterprise Architecture and Information Management, Information and Communications Systems, Corporate Support Division	P: 073635 3779 E: IMpolicies@dcs.qld.gov.au

Policy Owner:

Executive Director, ICS, Department of Community Safety.

Glossary:

Refer to the Department's Information Security Policy glossary.