Post-separation employment

In this advisory:

Introduction

With the workforce becoming more mobile, employees moving to another organisation are increasingly likely to be using their skills and knowledge in a related or even a competing organisation. This increases the likelihood that issues of undue influence, conflict of interest and information security may arise when employees leave a government agency to pursue related opportunities in the private sector. This can create significant risks for government agencies' business and reputation.

Under s. 70 of the The *Integrity Act 2009,* former senior government representatives are prohibited from making any contact which attempts to influence state or local government decision making in any area in which they had official dealings during their last two years in office.

The Public Service Commission's Directive No. 2/09, *Employment separation procedures* (PDF, 47 kB) requires that public service departments and offices have procedures in place to manage the risks when employees leave the organisation.

Major misconduct risks

Risks of misconduct are most likely to occur when employees move from a government agency to a private sector organisation that:

- operates in a related field or competes commercially with the government agency
- receives contracts, funding, loans or similar from or through the agency
- comes under the licensing, regulatory or auditing authority of the agency
- engages in lobbying ministers, members of parliament or government agencies.

Government agencies in such situations are exposed to three broad categories of risk — undue influence, conflicts of interest and information security.

Undue influence

The integrity and reputation of a department can be tainted by a single incident that calls into question the fairness or impartiality of a process or of decisions made by departing employees, either before or after they have left public sector employment.

For example:

- departing employees' decisions on behalf of either employer may be biased as a result of the new relationship
- departing employees may communicate confidential information to the new employer, thus giving them an unfair advantage over their competitors
- former colleagues of the departing employee may give special treatment to them or their new employer.

Conflicts of interest

A conflict of interest arises when a public official's private interests could improperly influence the performance of their official duties. Actual and potential conflicts of interest always need to be identified, disclosed and effectively managed.

When an employee submits their resignation, this effectively amounts to a declaration of a potential conflict of interest as it means that their knowledge and skills will be available to another organisation. In these circumstances, there is a risk that they may:

- misuse resources such as phones, email, stationery, vehicles, equipment and work time for non-agency purposes
- direct or persuade other staff to misuse resources for non-agency purposes to benefit or impress their prospective employer
- make or influence decisions to benefit or impress their prospective employer
- form irregular and possibly improper networks of friends which circumvent official communication and information channels.

Read more about conflicts of interest.

Information security

Information is property, and it must always be regarded as a corporate asset. It differs from physical assets in that it is harder to put a price on and, once stolen, can be difficult to recover from those who have benefited from it.

The loss or misuse of confidential official or commercial information as a result of poor information security can damage an organisation's reputation, business activities and profitability. If the public loses confidence in the integrity of an agency's processes and decisions, people may be less willing to participate in its legitimate attempts to gather information.

Types of information open to misuse include:

- information protected by law, convention, or the *Queensland Government information security classification framework* (DOC, 690 kB) (e.g. Cabinet-In-Confidence documents)
- commercial information (e.g. trade secrets, research, technical processes, information about competitors' business activities, client information to generate business leads)
- sensitive information about proposed changes and policies (e.g. political, industrial, legislative, regulatory or zoning)
- information provided to the agency in confidence (e.g. tenders, development proposals)
- personal information protected under the *Privacy Act 1988* (Cwlth) (e.g. personal particulars and identity data, health information, criminal records)
- copyright materials and other intellectual property (e.g. technical inventions, manuals, artworks, journal articles, scientific results, teaching materials, statistics, survey results).

Departing employees put information and intellectual property at risk when they:

- provide particular documents, research findings or materials in order to impress or win favour with a new or prospective employer
- collect information and materials they think may be useful to them in their new role and take them to the new workplace
- mistakenly believe that documents and materials which they had a substantial role in creating are in some sense their personal property, and take and use them in their new role
- contact former colleagues on a personal level requesting documents or information
- manipulate, conceal or destroy organisation information to benefit their future employer.

The most common avenues for unauthorised loss of confidential information are:

- taking or faxing hard copy documents
- emailing electronic files
- downloading electronic materials to memory devices (such as phones, CDs, USBs and laptops)
- retaining remote access to the computer network after separation.

Strategies to prevent misconduct

Given that a certain number of employees can always be expected to leave government for private sector employment, the most effective way of minimising potential harm is to foster ethical conduct throughout their period of employment. The following steps will help you to anticipate, minimise and manage risks before, during, and after separation.

Assess the risk

You are advised to conduct a detailed risk assessment along the lines indicated in the previous section. Obviously the risks will vary depending on the departing employee's role and classification, with the positions most at risk being chief executive officers, senior officers, and other key positions.

Routinely review your risk assessment, and continually revise and manage identified separation risks.

Implement policies and procedures

Once you have identified the risks, put strategies, policies and procedures in place to manage them. Under Directive No. 2/09, *Employment separation procedures* (PDF, 53.1 kB), if you are employing staff under the Public Service Act, you must have established employment separation procedures in place.

Under Principle 3, 'Human resources management' of the Queensland Government Information Standard 18 *Information security* agencies are required to develop and implement procedures for the separation of employees from, or movement within, the agency, to maintain the security of information.

Consider developing policies and procedures and training programs that cover the following.

Normal employment

- Ensure that security vetting, declarations of interests and criminal history checks are carried out before people are appointed to positions with access to sensitive information.
- Limit job offers by including contract clauses restricting successful tenderers from employing agency employees who managed or were materially involved in the tender process (for a specified period during and after the process).
- Require certain employees to declare job offers in accordance with s. 6.5 of the *Public Service Commission Directive No. 3/07* (PDF, 58 kB).
- Maintain registers of interests.
- Improve information security.
- Promote awareness of confidentiality requirements.

Pre-separation

- Introduce a separation declaration that reminds departing staff of their obligations regarding conflicts of interest, post-separation restrictions and lobbying.
- When an officer gives notice, make it their manager's responsibility in each case to ensure that there are no actual or perceived conflicts of interest.
- Remind employees that giving notice does not end their obligation to declare any possible conflict of interest and to cooperate in managing it.
- Develop a separation checklist to ensure that identification cards, agency equipment and official documents are returned and computer network rights are revoked.

Post-separation

- Consider introducing contractual provisions preventing senior officials, or other officers in positions where there is a serious risk or sensitivity, from taking employment in specific fields during a fixed period or time after leaving your agency.
- Ensure that staff are aware of the legal restrictions on post-separation dealings with the agency.

Align with your code of conduct

Ensure that your agency’s code of conduct includes clear statements of employees’ obligations regarding:

- putting the public interest above all private interests
- declaring conflicts of interest
- post-separation employment
- separation processes, including management of potential conflicts of interest
- information security
- contacts and dealings with lobbyists
- gifts and benefits

- leading by example.

Promote training and awareness programs

Ensure that key issues are not simply covered at induction and then forgotten. Instead, provide periodic reminders and refresher training. For example, when a departing staff member goes to a client organisation, business or competitive industry, remind remaining staff that the departing employee is to be given no better treatment or service than any of your agency's other clients.

It is important to educate your staff on the policies and procedures that may affect them directly when they leave your employment, especially their obligations in regard to conflicts of interest, lobbying and information security.

Maintain high ethical standards

At present there is very little to discourage other organisations from trying to gain advantage in their dealings with government, as long as they stop short of criminal activity such as bribery or fraud. A strong reputation for integrity (led by example and enforced promptly, fairly and firmly) is the best defence against future misconduct.

On the other hand, government agencies — particularly when trading in commercial competition with other organisations — should guard against benefiting improperly from confidential information possessed by employees recently recruited from the private sector by maintaining high standards of ethical conduct. Publishing and promoting such standards will help to reassure the public that the government sector can be relied on to behave ethically.

Further information and resources

- Crime and Misconduct Commission & Independent Commission Against Corruption 2004, *Managing conflicts of interest in the public sector: guidelines* (PDF, 345 KB)
- Crime and Misconduct Commission & Independent Commission Against Corruption 2004*, Managing conflicts of interest in the public sector: toolkit* (PDF, 2 MB)
- Crime and Misconduct Commission 2008, *Public duty, private interests* (PDF, 2 MB)
- *Criminal Code Act 1899* (Qld)
- *Integrity Act 2009* (Qld)
- *Public Sector Ethics Act 1994* (Qld)
- *Public Service Act 2008* (Qld)
- Public Service Commission 2009, Directive No. 2/09, *Employment separation procedures* (PDF 45 KB)

Please contact us if you would like further detailed guidance and information on any aspect of this advisory.

Last updated: 15 April 2013

Contact us
Phone: (07) 3360 6060 or 1800 061 611 (toll-free in Queensland outside Brisbane)
Email: mailbox@cmc.qld.gov.au