# Information privacy breach checklist – for contracted service providers

This checklist has been developed for use by Contracted service providers (CSPs) when notifying the Department of Families, Seniors, Disability Services and Child Safety about a privacy breach.

It should be read in conjunction with the Office of the Information Commissioner (OIC) guideline.

The department cannot provide advice about how a CSP should respond to a breach, so CSPs should consider whether to seek independent advice from the OIC or a legal advisor.

## *What happened?*

Please provide a summary of what occurred, including what information was involved.

[Insert details]

## *Step 1: Containment*

What containment action has been taken? Has it contained the breach? *For example:*

- *email successfully recalled*
- *recipient confirmed email deleted from Inbox and Trash and not shared with anyone else*
- *hard copy records retrieved*
- *password protected device wiped remotely*
- *system access revoked; system access codes revoked*
- *legal advice or police assistance sought to retrieve information*

[Insert details]

## *Step 2: Risk assessment*

A risk assessment should be conducted, to inform the next steps. *For example:*

- *What personal information was involved and how sensitive is it? e.g. medical details or training list*
- *Who is affected by the breach and what are their circumstances? e.g. high-profile person*
- *What is the context? e.g. address of DFV victim given to former partner, or to brother*
- *What was the cause and extent of the breach? Do any protections or mitigations apply?*
- *Is there a risk of harm to the individual? e.g. physical, financial, reputational damage*
- *Is there a risk of harm to the department/CSP? e.g. reputational damage; regulatory penalties*

**Does the use or disclosure of this information create a risk of harm to anyone?** **Yes** **No**

[Insert details]

## *Step 3: Notification*

Consideration should be given to who should be notified. *For example:*

- *Have senior managers in the CSP been notified?*
- *Should police be notified? (e.g. if it involves theft)*
- *Should the Queensland OIC be notified? NB: data breach notification is not mandatory in Queensland.*
- *Should the OAIC be notified? NB:* Privacy Act 1988 *(Cth) does not apply to contracts with State government agencies, but may apply to certain types of information e.g. TFNs*
- *Should affected persons be notified (see below)?*

### Notifying affected persons

Each incident should be assessed on its facts, but it is expected that affected persons will be notified if there is a risk of harm, or if there is any action the person could take to minimise harm.

*Relevant considerations include:*

- *What is the risk of harm, loss, or damage to the individual? For example:*
  - *Is there a risk of identity theft or fraud?*
  - *Is there a risk of physical harm, stalking or harassment?*
  - *Is there a risk of humiliation or damage to the individual's reputation?*
- *What is the likelihood of the harm occurring?*
- *What is the ability of the individual to avoid or mitigate possible harm?*
- *Is there a likelihood that being notified might cause the affected individual more distress than it would alleviate (particularly if there is little risk of harm)?*

Generally, the CSP will be responsible for notifying affected individuals. Guidance about what should be included in the notification is available on the OIC website.

[Insert details]

## *Step 4: Preventing future breaches*

Consider what caused the breach and how it could have been prevented. Have you taken action to prevent a recurrence? *For example:*

- *improved physical or technical controls*
- *review information handling policies and procedures*
- *review staff training and completion rates*
- *is disciplinary action appropriate?*

[Insert details]

## *Other information*

Is there any other information the department should be aware of?

[Insert details]