Policy and Procedure Register updates

Summary of changes to:

Information security procedure

1. **Reason for new/updated policy or procedure** *(select all that apply)*		
☐ Change of policy/procedure requirements	☐ Audit/review recommendation	
☐ Change to legislation/delegations	☒ Due for review	☐ Other

The Information security procedure (the procedure) was due for review on 1 June 2020. Updates have been made to simplify the process for employees to apply security classifications, protect information and report incidents or breaches.

The updates aim to provide employees with clear examples of how they must protect information as well as when and how to respond to an information security incident or breach.

This procedure is supported by the Information security guideline.

2. Summary of changes

The procedure has been updated to align with PPR requirements.

The process sections within the procedure have been condensed into 4 sections which are:

- Determine the information security classification (formerly ICT security)
- Apply and control the information security classification (formerly Applying information security classifications)
- Protect information (formerly Protecting information and Malware and malicious code prevention)
- Respond to information security incidents and breaches (formerly Breach of security and Reporting ICT security incidents).

The Protect information section has been rewritten to provide employees with clear, actionable steps to protect information, including malware prevention and clear desk/clear screen practices.

The Responding to information security incidents and breaches section now includes privacy data breaches.

Inclusion of a new Information security classification tool will assist employees in the classification of information assets to align with the Queensland Government's Information Security Classification Framework (QGISCF).

3. Impacts to roles and responsibilities

Does the new/updated content change staff roles/responsibilities *in any way*?	☒ Yes	☐ No
If yes, select the type of change: *(select all that apply)*		
☒ Revised responsibilities	☐ New/additional responsibilities	☒ Removed responsibilities

Position title	**Summary of change**	**Page#**

Employees	Employees now must report suspected or discovered privacy breaches. Some key process responsibilities were missing from the previous version of the procedure. These have now been included but do not represent new obligations.	4
System security administrators	Direct responsibilities for the prevention of malware and malicious code have been removed from this procedure and will now be outlined in the new iSecurity website.	5
Information Security Services unit	Direct responsibilities for protecting information have been removed from this procedure and will now be outlined in the new iSecurity website.	3-4
Enterprise Technology Services unit	Direct responsibilities for monitoring the system's capacity have been removed from this procedure and remain a business unit responsibility.	

4. Communication and support for implementation

Changes to the procedure have been communicated with the relevant internal stakeholders, with consultation conducted across the department, including input from subject matter experts and relevant directors within the Digital Innovation Division (DID).

Department wide communication via OnePortal and ConnectEd will be developed in consultation with the DID communication team.

For further assistance, please contact:

- Policy/procedure contact:

  Governance Risk and Compliance Unit
  Email: ictpolicy@qed.qld.gov.au