2019

THE LEGISLATIVE ASSEMBLY

FOR THE AUSTRALIAN CAPITAL TERRITORY

CANBERRA INSTITUTE OF TECHNOLOGY

ANNUAL REPORT 2018

CORRIGENDUM

Presented by

Andrew Barr MLA

Minister for Tertiary Education

CORRIGENDUM

2018 CIT ANNUAL REPORT

Supplementary information for the 2018 CIT Annual Report tabled out-of-session on 15 April 2019.

Section B.3 Scrutiny of the Annual Report Directions requires *public sector bodies must report on progress during the reporting period in relation to undertakings made in reports that are produced by directorates charged with responsibility for scrutiny, including the Auditor-General, ACT Ombudsman and Legislative Assembly Committees*.

Two Auditor-General performance audit reports relating to CIT were tabled in 2018. These were:

1. ACT Government Strategic and Accountability Indicators Report No.2/2018 (Report released 1 February 2018, Government Response tabled 5 June 2018); and
2. 2016-17 Financial Audits Computer Information Systems Report No.4/2018 (Report released 28 February 2018, Government Response tabled 31 July 2018).

This information should have been included on page 48 of the 2018 CIT Annual Report.

ACT Government Strategic and Accountability Indicators Report No2/2018		
Recommendation	**Government Response**	**Status**
Recommendation 2 Strategic Indicators should be improved by Canberra Institute of Technology by removing or amending strategic indicators so they fully meet the criterion of *Representative.*	**Agreed in principle.** Existing indicators will be reviewed in line with updated guidance material once it has been released. Amended indicators will be phased in from the 2019-20 Budget.	**On-going.** CIT is now reviewing its Strategic and Accountability Indicators with a view to agreeing a revised set prior to January 2020

2016-17 Financial Audits Computer Information Systems Report no.4/2018		
Recommendation	**Government Response**	**Status**
Recommendation 5 The Canberra Institute of Technology, should: a) remove all generic (shared) user accounts and assign all users with a unique user name and password; b) require passwords for generic (shared) user accounts to be changed every 90 days in accordance with the ACT Government's	**a) Not Agreed.** **Complete**. Whilst the use of generic accounts are kept to a minimum there are sound business reasons why generic accounts are required in specific circumstances. To mitigate risks associated with generic account use an audit of generic user accounts was completed in September 2017 leading to the removal	**Complete.** Additionally, there is a significant project underway to modernise the ICT environment for CIT, which involves transitioning away from the Micro Focus (formerly Novell) infrastructure to Microsoft platforms. During this project, all user accounts (personal, generic or shared) will be reviewed and provisioned in the new CIT domain based on operational requirements and in accordance to the Shared Services ICT security framework.

Password Standard; and c) implement alternate secure network logon methods (in consultation with Shared Services ICT) that facilitate fast access to systems, where such access is required. This may include, for example, swipe card or biometric (e.g. fingerprint or facial recognition) readers.	of some generic accounts. The Generic Account Request Form has also been revised to require the approval of the Directorate's CIO as part of ongoing business improvement activities. The Whole of Government User Identity Policy has also been revised to require approval of Directorate CIOs for any new generic accounts. This policy has been promulgated through the Shared Services Website. **b) Not Agreed. Complete.** ACT Government will investigate clearly identifying those accounts that are used by business systems to function as part of its ongoing business improvement activity. The password "set never to expire" will remain. **c) Partially Agreed. Complete.** In prior years, Shared Services ICT has advised the Audit Office of other forms of access that have been considered, such as 5 the progressive implementation of the Imprivata simplified logon solution. However, the use of alternate solutions is based on the business areas risk versus	

	benefit analysis. Many of the generic accounts are only activated during specific events (e.g. disasters or when undertaking specific tasks such as testing and training). As such, implementing an expensive solution may not be warranted. Determination will be made on a system-by-system basis.	