MINISTRY OF SOCIAL DEVELOPMENT
TE MANATŪ WHAKAHIATO ORA

Report

Date: 6 April 2017 **Security Level:** Sensitive

To: Hon Anne Tolley, Minister for Social Development

Issues with use of Government shared workspace for collection of client level data

Purpose of the report

1 To provide you with a summary of the issues that led to the decision to shut down access by providers to the Government (run by Department of Internal Affairs) shared workspace for collection of client level data, and provide you with information on the actions that have been taken and the next steps.

Recommended actions

It is recommended that you:

2 **note** the issues that led to the decision to shut down access by providers to the government shared workspace for collection of client level data

Yes/No

3 **note** the immediate actions that have been taken to address the folder access issues

Yes/No

4 **note** that the Department of Internal Affairs (DIA) has engaged an independent third party to assess the event logs to fully understand the access and activity around this issue and that we will keep you up to date with progress of this review

Yes/No

5 **note** that I have agreed with the Chief Executive of the Ministry for Vulnerable Children, Oranga Tamariki, that she will also report back to you by next Thursday 13 April on the process and timeline for considering and recommending a secure and robust alternative to the current system

Yes/No

6 **note** that I will be commissioning an independent review of the system implementation and will provide you with further advice on this once the Terms of Reference have been agreed. These Terms of Reference will be agreed by the Government Information Security Officer.

Yes/No

Brendan Boyle
Chief Executive
Ministry of Social Development

6/4/17
Date

Hon Anne Tolley
Minister for Social Development

11-4-17
Date

Background

7. To implement the collection of client level data from 1 July 2016 and 1 July 2017 we elected to use the government Shared Workspace as a way for providers to upload spreadsheets that contained their individual client level data.

8. This was an interim solution while we developed a permanent system to collect this data, and we have been working concurrently on that more permanent solution.

9. Providers are each given a library in the shared workspace where they can upload their spreadsheet containing the client level data. Each provider should only have permission to see their own library, with the Ministry being able to see all libraries.

10. There was an issue of a provider having access to another provider's library and as a result of this, actions were undertaken to address this.

Summary of Issues

11. In January 2017 there was a default "shared library" that all users could access. This is a standard feature of the shared workspace environment. One provider uploaded an Individual Client Level Data (ICLD) spreadsheet with data in it into this library in error.

    We were advised of the existence of a spreadsheet in the shared library by another provider and immediately moved that spreadsheet to the relevant provider's library. We than disabled all permissions to the shared library. We reviewed the access information we had and confirmed that the last user to have opened that spreadsheet was the provider who uploaded it. As such there is no evidence that anyone else looked at the data.

12. At 11.44pm on Friday 31 March, a Building Financial Capability provider emailed a Ministry staff member that they could see another provider's library. The other provider's library belonged to another Building Financial Capability Provider. There was nothing, i.e. no client level data, in the library.

13. On Monday morning we reviewed the permissions for the provider and found that all other providers had permission to view its library. We immediately turned off the other providers' permissions and reviewed all other libraries to ensure that only each individual provider and the Ministry had permission to view their own library. In removing the permissions we inadvertently turned our own permission off.

14. We instructed **9(2)(ba)(ii) - Commercially Sensitive** (who manages the shared workspace) to reinstate only our permission over the library and they confirmed they had done that on Monday at 3.54pm. It appears **9(2)(ba)(ii) - Commercially Sensitive** had given every provider permission to view the original provider's library. **9(2)(ba)(ii)**

15. We discovered this error at 8.04am on Tuesday morning when a Regional Manager advised National Office that one of their providers could see the provider's library. We immediately turned off these permissions and again reviewed all other libraries to ensure that only the provider and the Ministry had permission to view their own library.

16. The analyst managing provider information has been regularly checking what data has been uploaded to the shared workspace to check on its quality. To the best of his knowledge no data has been uploaded to the provider's folder throughout this period.

17. A detailed incident timeline is provided in Appendix One

Immediate incident management

18. We contacted DIA on Tuesday 4 April to ask them to restrict all access to the libraries on our shared workspace. DIA confirmed that as of 9pm the same evening no providers could access their folders.

19. On 5 April a message was added to the shared workspace to say 'We are currently undertaking technical assessment on this portal and it is unavailable until further

notice; please retain any data you were planning to upload onto this platform in the meantime.'

Communication to stakeholders

20. We made contact with the provider who notified us of the April issue, reiterating the above point, and thanking them for their notification. We have also contacted the affected provider and made them aware of the incident and apologised for it happening.

21. The Media Statement released by the Minister was sent to all providers at the time of release yesterday.

22. We will prepare further communications to providers on the timeframes for the new IT platform once we have revised our plan. In the interim we will reiterate our expectation that Phase One providers continue to collect client level data, and our intention to introduce the ICLD contract clause from 1 July 2017 for all relevant providers.

Due Diligence on collection of ICLD for 2016 data collection

23. The following is the due diligence on the process for the collection of individual client level data:

23.1 Material was sent to providers in July 2016 and November 2016 and included the template to be completed, instructions on how to upload the completed template into the Shared Workspace and asking for a nominated person who would be given access to the Shared Workspace to upload the spreadsheet. The provider was responsible for ensuring the nominated person established a RealMe account and the Ministry gave that account the relevant permissions within Shared Workspace.

23.2 Before we communicated with providers, and before we engaged in an agreement with DIA to use the Shared Workspace we undertook a Security Risk Assessment covering the use of the Shared Workspace for the purposes of providers uploading the ICLD spreadsheets.

23.3 The Security Risk Assessment identified and assessed the security risks associated with the use of the system, which includes the identification of the controls used to mitigate these risks. This was signed off on 22 November 2016. It has two parts to it:

i. Certification – the SRA was certified by the Chief Information Security Officer, who confirmed that the risk assessment was an accurate and complete picture of the risks and provided comment on the acceptability of the risk, based on information available at the time

ii. Accreditation – The Business owner (the responsible Deputy Chief Executive) accepted the risks before the system was purchased.

23.4 As the April collection date approached we revisited the Security Risk Assessment to ensure that it was still a fair reflection of the risk environment. This was done on the basis that we knew more about how the programme would operate. As a result the Security Risk Assessment was updated and was to be re certified and accredited this week. The revised Security Risk Assessment raised some concerns that the Shared Workspace was not a fit for purpose solution given the level of risk associated with the ICLD programme.

24. Both Security Risk Assessments relied on the Shared Workspace's security certification that had been completed by DIA, but supplemented with the additional activities unique to the Ministry's use of the shared workspace. The controls were in the process of being verified to support the certification and accreditation of the revised Security Risk Assessment, but they were not verified as part of the original Security Risk Assessment (as the level of risk didn't warrant this under the Ministry's Certification and Accreditation process).

Provider Statistics and direct system costs

25. The total number of providers involved in Phase 1 is 153 providers and 384 users have been granted access to the shared workspace thus far from 136 providers (so there are multiple users for each provider including Ministry users).

26. 109 users from 72 providers and the Ministry Administration team have actually logged into the system since the site went up.

27. There are 10 providers who had uploaded a file to the shared workspace, all of whom are Building Financial Capability providers.

28. The total amount spent on the data system to date is $2,750.

Next steps

29. The Department of Internal Affairs (DIA) has engaged an independent third party to assess the event logs to fully understand the access and activity around this issue and we will keep you up to date with progress of this review.

30. I have agreed with the Chief Executive of the Ministry for Vulnerable Children, Oranga Tamariki, that she will also report back to you by next Thursday 13 April on the process and timeline for considering and recommending a secure and robust alternative to the current system.

31. I will be commissioning an independent review of the system implementation and will provide you with further advice on this once the terms of reference have been agreed. These Terms of Reference will be agreed by the Government Information Security Officer.

Appendix One: Detailed Incident Timeline

Friday, 31 March

9(2)(ba)(ii) emailed 9(2)(a) planning and reporting at 11:44pm on Friday the 31st of March. This was to inform the Ministry they can see another 9(2)(ba)(ii) document folder. There was no content within this folder.

Monday, 3 April

At 8:42am on Monday the 3rd of April 9(2)(a) forwarded this on the analyst within the reporting team to enquire and fix the permissions issue.

The analyst viewed the library permissions for 9(2)(ba)(ii) and found that all user groups had permission to see this documents folder.

The analyst removed permissions for all but 9(2)(ba)(ii) from the documents folder. In doing so the analyst had also removed the Ministry's permissions.

Further to this action, the analyst was tasked with checking all permissions in all provider folders to ensure only those appropriate had access. This was completed in the morning, and no other errors were found. 9(2)(ba)(ii)

The analyst contacted the help desk at 2:37pm via email to reinstate permission for only the Ministry administration group to view the 9(2)(ba)(ii) documents folder. 9(2)(ba)(ii)

The employee responded at 3:54pm confirming that the 'community investment-level data owner' (the Ministry administration group) has been given full access.

Tuesday, 4 April

At 8:04am on Tuesday the 4th of April a regional contract manager contacted 9(2)(a) to inform the Ministry that their provider can see 9(2)(ba)(ii) document folder.

At 8:52am this email was forwarded onto the analyst immediately to sort. The analyst went back into the system and discovered that all user groups were able to see 9(2)(ba)(ii) document folder.

The analyst deleted all permissions immediately upon reading the email that morning for all but the Ministry's admin group and 9(2)(ba)(ii) user group.

- This was then double checked by another Analyst in the team to ensure this was completed.
- Further to this the second analyst checked all the other libraries again for to ensure security.

Throughout this period, the analyst has been regularly checking what data has been uploaded to the shared workspace; to the best of his knowledge no data has been uploaded to the 9(2)(ba)(ii) folder