The Highland Council

Agenda Item	
Report No	

Adult & Children's Service Committee
21 August 2013

Audit Action Plan: Care First

Report by Director of Health & Social Care

Summary

This report details the actions taken to address the Service specific issue raised by Internal Audit regarding the re-use of previous passwords in CareFirst.

1. Background

1.1 CareFirst is the case management system for adult services, children's services and criminal justice. The system went live in 2007 and has around 800 registered users. The system is under continuous development and was recently updated with the addition of a finance module. Nationally, it is used by around 110 social care organisations.

2. Audit Findings

2.1. The findings of the audit review are detailed in Annex A and Annex B. The findings fell into 2 groups – those requiring action by the Service and those requiring action at a corporate level. Although the audit identified that the majority of necessary password controls were in place, it was noted that it was possible to re-use previous passwords in CareFirst.

2.2 The re-use of previous passwords is recognised as poor password practice, and many systems have the facility to prevent this. CareFirst does not have this facility. CareFirst passwords are force-changed every 3 months. A new password must be entered at that point. However, it would be technically feasible, for a user who was determined to do so, to replace the force-changed password back to the previous password. There is no evidence that this happens, but the system does provide the opportunity to do so.

2.3 Members should note that users must also logon to the Highland Council network before CareFirst can be accessed. Passwords for the Council network are force-changed every 6 months, which provides an additional level of security.

3. Action Taken To Address the Findings

3.1 It is not possible to effect this change in CareFirst locally, and the Council is dependent on the system supplier to make this change. We were originally informed that the change would be implemented in the next CareFirst upgrade. However, it was clear post-upgrade that this facility had not been implemented.

3.2 We now have an assurance that this facility will be provided by January 2014. That does involve a further delay, but it should be borne in mind that this is a change that would affect all organisations using CareFirst, not just the Highland Council and NHS Highland. In the meantime, both network passwords and CareFirst passwords will continue to be force-changed regularly, and users will be reminded to follow good password practice.

4. Implications

4.1. **Resource Implications**
If, as expected, the provision of this facility is rolled out as part of a CareFirst upgrade, there should be no additional resource implications, other than those to be expected as part of the upgrade process.

4.2. **Legal, Equalities, Climate Change**.
No implications.

4.3 **Risk implications**
Users can re-use previous passwords. Users are being reminded of the requirement to follow good password practice.

Recommendation

Members are asked to note the content of the audit report, and the proposed solution to address the issue raised.

Bill Alexander
Director of Health & Social Care

Date: 8 August 2013

Author: George McCaig, Head of Care Support

Appendix 1: AUDIT REPORT SUMMARY

Health and Social Care Service / Chief Executive's: CareFirst (Follow Up)			
Report No.	**Type of Audit**		**Issue Date**
HG46/003.bf	Computer	**Draft Report**	30/01/13
		Final Report	18/03/13

1. Introduction

1.1 A computer audit report of the CareFirst Social Care Case Management System used to record details of adult and children's services was issued on 18/11/10. Since the original audit was undertaken, some Council staff members have transferred to NHS Highland as part of the integration project between the Council and NHS Highland. These NHS staff still use the CareFirst System.

1.2 This report reviewed three areas of the system, namely:

(i) How physical and logical access to it was controlled
(ii) Whether it was operating as an effectively controlled application in relation to areas including the processing of input documents and output reports
(iii) How the system had been implemented.

1.3 The report concluded that the implementation of CareFirst System had been satisfactory, but additional controls were required in relation to access and the operation of the application. The following key areas were identified for improvement:

- A corporate mobile computing policy was required to identify the appropriate security measures for mobile computing and taking personal data off site.
- The CareFirst Access Control Policy needed to be finalised and made operational. All user CareFirst System access privileges should be periodically reviewed. Special users with fixed access privileges that reflect the 14 job roles should be set up and used as a basis for creating new users.
- A corporate access control policy on the use of network services should be formulated in order to comply with the guidance in ISO 27002. ICT Services should work with Fujitsu Services to make it transparent to data owners within the Council who has access to shared network folders. ICT Services should also work with Fujitsu Services to ensure audit trails are set up of access to shared network folders that contain confidential data. They should be monitored and evidential assurance provided to data owners within the Council that no unauthorised access is taking place.
- The ongoing data quality assurance exercise being carried out by the Health and Social Care Service with regard to CareFirst data should be continued to provide assurance that the CareFirst data is complete, accurate, and up to date.
- Health and Social Care staff should continue to raise the requirement for relational database table diagrams and a catalogue of fields from supplier at the CareFirst User group. ICT Services should provide corporate guidance on sending emails containing personal information to external recipients who do not have access to GSX.

1.4 The Action Plan, completed by the Team Leader (Projects and Technology) and the ICT Delivery Manager showed that the actions to address the above control weaknesses would be addressed by the end of April 2011.

1.5 This follow up audit was undertaken as part of the annual plan for 2012/13 to ensure that the management agreed actions from the previous audit have been completed.

2. Review Objectives

The objectives of the review were to ensure the management agreed actions had been satisfactorily completed with regard to:

2.1 Physical and logical access control are sufficiently robust

2.2 The CareFirst application operates effectively.

3. Main Findings

The main findings of the review, referenced to the above review objectives, are as follows:

3.1 This objective has only been partially achieved. A corporate mobile computing security policy has been produced and published on the Council's intranet. The CareFirst Access Control Policy is now finalised and all user access privileges are now periodically reviewed. A group facility within the CareFirst System now means that new users are set up by copying the access privileges of existing users with a similar job role. However, corporate third party access guidelines have not yet been produced. The revised completion date is 30/06/13. Users are not yet prevented from re-using previous passwords. The revised completion date is 30/04/13. A corporate network access control policy has not yet been produced. Corporately data owners within the Council are not informed as to exactly who has access to their shared network folders. Audit trails are not set up to show access to shared network folders that contain confidential data. Audit trails are not monitored and evidential assurance is not provided to data owners to show that no unauthorised access is taking place. The revised completion date is 30/06/13.

3.2 Again this objective has only been partially achieved. The ongoing data quality assurance exercise provides assurance that the data is complete, accurate, and up to date. As recommended, Health and Social Care members of staff have raised the requirement for relational database table diagrams and a catalogue of fields from supplier at the CareFirst User group. Unfortunately the supplier has not provided this and staff cannot take this action any further. The CareFirst table level audit trail is switched on and the problem regarding the availability of Children's Plan Report in the CareFirst system is resolved. However, ICT Services have not yet provided corporate guidance to staff on sending emails containing personal information to external recipients who do not have access to the government secure extranet. The revised completion date is 28/02/13. ICT Services have not yet written to the supplier to obtain assurance for the Health and Social Care Service that database administrator activity is audited, monitored and controlled. The revised completion date for this is 28/02/13.

4. Conclusion

4.1 A significant amount of progress has been made against the actions by Health and Social Care staff particularly around finalising the Access Control Policy, data quality assurance and the activation of the table level audit trail. The progress against actions by ICT Services has not been so good, but the recommendations made with regard to ICT Services were more demanding because they required the production of corporate ICT policy relating to information security matters. In addition progress has been delayed because the previous Senior Information and Security Officer was on sick leave for a prolonged period prior to leaving the Council and the post remained vacant for a period prior to being filled. A new Senior Information and Security Officer has recently been appointed and the outstanding actions should be completed by the revised dates.

4.2 There are 5 recommendations in this report. One is classified as high priority and four are classified as medium priority. All of the recommendations are due to be implemented by 30/06/13.

5. Audit Opinion

5.1	The opinion is based upon, and limited to, the work performed in respect of the subject under review. Internal Audit cannot provide total assurance that control weaknesses or irregularities do not exist. It is the opinion that **Limited Assurance** can be given in that weaknesses in the system of controls are such as to put the system objectives at risk, and/ or the level of non-compliance puts the system objectives at risk.

Appendix 2

The Highland Council

Agenda Item	
Report No	

EXTRACT FROM Audit and Scrutiny Committee – 20th June 2013

Updates of Actions Arising from Internal Audits of Fuel Cards, CareFirst and Business Community Planning

Report by the Head of Internal Audit & Risk Management

Summary

This report provides Members with an update of the progress in implementing the actions arising from three reports which were presented at the last meeting on 28th March 2013.

1. Background

1.1 At the last Audit & Scrutiny Committee of 28th March 2013 Members were presented with eight final Internal Audit reports, of which three were follow up reports. In view of the limited assurance given to two of the follow up reports and the numbers of actions still to be completed, Members requested that a report should be submitted to the next meeting in order to confirm that the recommendations had been completed satisfactorily. The reports concerned are as follows:

- *Administration of Fuel Cards (follow up)*
- *CareFirst (follow up).*

In addition, Members also requested an update with regard to the following review in view of the limited assurance given together with the high number of actions to be completed:

- *Business Continuity Planning.*

2. Updates of Actions Arising

2.2 <u>CareFirst (follow up)</u>

The actions taken to date are provided at appendix 2 which shows that the high priority action has been addressed and that two medium priority actions now remain outstanding as follows:

(i) Section 3.1.3 refers to the production of corporate third party guidelines which have now been incorporated within the ICT User and Network Control Policy. However, to comply with ISO 27001, there needs to be a process to ensure that all third parties are made aware of the Council's information security policies. An Information Security Policy is due to be

completed by the end of June 2013. It is necessary for ICT Services to review all ICT contracts, including those resulting from software procurements by other Services, e.g. Phoenix e1 system and Axise Pensions system, to ensure non-disclosure agreements are included. This is now in progress and the ICT Delivery Manager has contacted the Procurement Section to ensure that it specifies, in their procedures, that ICT Services need to review any ICT related procurement contract.

(ii) *The original audit report on CareFirst gave positive assurance that the majority of good practice password controls are in place within the system. However, it was highlighted that the system did not have the facility to force users not to re-use their existing password. Although this action has been progressed by the Health & Social Care Service Team Leader (Projects and Technology), it is dependent upon a new software release from the supplier which will be available by January 2014. In the meantime, passwords continue to be reset securely on a quarterly basis. Additional security is also provided through the need to access the Highland Council network before CareFirst can be accessed.*

3. Implications

3.1 ***Legal & Risk:*** *The implementation of the agreed actions referred to within the audit reports will reduce the risk exposure to the Council.*

3.2 ***Resource:*** *The introduction of a fuel monitoring system will require to be resourced by the Director of TEC Services.*

3.3 ***Finance:*** *The introduction of a fuel monitoring system will require to be resourced by the Director of TEC Services.*

3.4 ***Equalities:*** *There are no implications*

3.5 ***Climate Change:*** *There are no implications*

4. Conclusions

4.1 *This report shows good progress with regard to implementing the agreed actions referred to in the three Internal Audit reports.*

Recommendation

Members are asked to note the good progress in implementing the actions arising from three reports which were presented at the last meeting on 28th March 2013.

Designation: *Head of Internal Audit & Risk Management*

Date:
Author: *Nigel Rose, Head of Internal Audit & Risk Management*
Background Papers: