Information Security Checks (November) 2017/18

City of York Council

Internal Audit Report

Business Unit: Corporate and Cross-Cutting
Responsible Officer: Assistant Director, Legal and Governance
Service Manager: Information Governance and Feedback Team Manager
Date Issued: 13 March 2018
Status: Final
Reference: 10180/008

	P1	P2	P3
Actions	**0**	**4**	**0**
Overall Audit Opinion	Reasonable Assurance		

Summary and Overall Conclusions

Introduction and objectives

1.1 In accordance with the agreed audit plan for 2017-18, information security checks were undertaken in November 2017. The purpose of these checks is to assess the extent to which confidential, personal or sensitive data is stored securely and to ensure that data security is being given sufficient priority within council departments. This was the first of these checks in this audit year.

1.2 Previous checks conducted in 2016-16 (Sep-16 and Mar-17) gave an overall opinion of Reasonable Assurance. It was noted that the position had improved in the March 2017 checks but there remained items of personal, sensitive and confidential information left unsecured.

1.3 The agreed actions from the March 2017 checks included the implementation of a secure key storage system at West Offices and that further audit checks would take place in 2017-18 once this had been implemented. At the time of this audit, the secure key storage system had recently been implemented and was being used by 13 teams based in West Offices. These teams participated in piloting the system to ensure it worked well and the plan is to roll it out to all teams.

Scope of the Audit

1.4 As part of this audit the two main council offices, West Offices and Hazel Court, were visited. This was the tenth of these information security checks since the opening of West Offices in 2013 and the council-wide implementation of a clear desk policy. The large number of non council staff who share West Offices means it is important for each service to recognise that information must be held securely within their area of the building.

1.5 The buildings were visited after most staff had left for the day. This enabled auditors to assess the extent to which data is being left out overnight without appropriate security. Instances of information being left unsecured were recorded where these posed risks to the council, either because they contain personal or confidential information. Instances of general security weaknesses were also recorded.

1.6 The findings are summarised below and detailed findings are set out in the attached Annex 3.

1.7 A visit was also undertaken at 30 Clarence Street (a recently refurbished council building now being used to deliver young people's services, adult's mental health services and containing council staff and external partners) to review the security arrangements at that site. This visit was done during working hours by arrangement with the facilities manager.

Findings

2.1 Overall, there was little difference from the March 2017 checks. The majority of cupboards were locked and most of those that were unlocked did not contain sensitive personal information. However, there remained some areas where cupboards had not been adequately secured, some sensitive information was not adequately protected and both information and physical assets were vulnerable to theft.

2.2 The general areas where information was not kept secure and improvements should be made include:

- In West Offices some cupboards containing sensitive, personal or confidential information were unsecured. There was a small number of documents that were not stored in cupboards (i.e. on top of cupboards, on desks, in boxes under or around desks).
- At Hazel Court, some cupboards containing personal and sensitive information were left unlocked and some sensitive information was left on desks or on open storage (i.e. shelving).
- Across both sites, a number of council assets were left unsecured, including laptops, cameras and keys to properties and vehicles.

Whilst the Hazel Court site and building security provides protection against external breaches of information, reliance should not be placed solely on the perimeter security and sensitive information must also be protected from internal breaches.

It was apparent that some of the lockable storage at Hazel Court is broken and that some teams do not have secure storage so are using open shelving. New, more secure, storage will be obtained for Hazel Court. Once this has been provided it is important that strong messages are given regarding the need to use that storage to keep all personal, sensitive and confidential information locked away. This must be done each time and reliance not solely placed on perimeter security.

2.3 xxxxxxxxxxxxxxxx

- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

2.4 As well as the most serious items noted above, there were numerous other instances of personal or confidential information being left unsecured throughout both offices. Some of these were through individual documents being left out or one or more cupboards in an area not being locked.

2.5 All individual items of information found during these checks have been rated according to the level of risk they pose if this information was accessed inappropriately, disclosed or lost. All items recorded pose some risk and action should be taken to ensure all information is kept securely. Specific attention should be paid to those rated as medium and high risk in the attached detailed findings, Annex 3.

2.6 The arrangements for ensuring information is kept secure at 30 Clarence Street seemed reasonable and there were no concerns arising from this visit and the discussions with officers on site. Adequate physical security measures are in place and staff working from this building showed a good awareness of the importance of keeping information secure and their responsibility for doing so.

Overall Conclusions

3.1 The council remains reasonably well protected against accidental disclosure of information. The vast majority of information is stored in cupboards, cupboard doors are generally closed; the majority of cupboards were locked and the clear desk policy is largely adhered to throughout West Offices and increasingly so at Hazel Court. Access to West Offices and Hazel Court buildings is controlled, though at West Offices there is a risk of unauthorised access by people who legitimately have access to the building.

3.2 However, these information security checks have been ongoing for some years and following initial improvements it was disappointing to note that the results of these checks were no better than the previous round of checks in March 2017.

3.3 There remain improvements to be made to protect against deliberate unauthorised access by ensuring all personal and sensitive information is locked away across all areas of the council. Action is also required to ensure that confidential information (e.g. financial data) is kept securely.

3.4 It seems that not all areas of the council have sufficiently developed a culture and good habits that recognise the importance of securing data within each team area and recognition that all information held is an asset that needs to be protected. There also remains a reliance on perimeter security at Hazel Court.

3.5 A secure key storage facility is now available in West Offices and all teams should start using this facility and ensuring all cupboards within their team / service area are locked at the end of each day or when their area is unoccupied.

3.6 Overall, there is currently satisfactory management of risk but a number of weaknesses were identified. An acceptable control environment is in operation but there are a number of improvements that should be made. Our opinion of the controls within the system at the time of the audit was that they provided **Reasonable Assurance**.

Actions

4.1 Actions to address the weaknesses identified in this report are included in Annex 1 below.

Annex 1

Agreed Action 1

a) Ensure all teams use the secure key storage in West Offices.

b) Accompany this with strong messages regarding the importance of securing information and that it is everyone's responsibility.

Priority	2
Responsible Officer	Facilities Manager & Information Governance Manager
Timescale	31 May 2018

Agreed Action 2

a) Provide sufficient lockable storage for teams based at Hazel Court.

b) Install secure key storage facility at Hazel Court.

c) Accompany this with strong messages regarding the importance of securing information and that it is everyone's responsibility.

Priority	2
Responsible Officer	Facilities Manager & Information Governance Manager
Timescale	31 May 2018

Agreed Action 3

a) Detailed findings will be fed back to individual service areas where information found was of a personal and sensitive nature (i.e. priority 1 and 2 findings in the spreadsheet attached at Annex 3).

Priority	2
Responsible Officer	Veritau Audit Manager / GRAG
Timescale	31 March 2018

Agreed Action 4

Further information security checks will be conducted by Veritau early in the 2018-19 audit year to check on progress once all teams are using the secure key storage.

Priority	2
Responsible Officer	Veritau Audit Manager
Timescale	31 May 2018

Audit Opinions and Priorities for Actions

Audit Opinions	
Audit work is based on sampling transactions to test the operation of systems. It cannot guarantee the elimination of fraud or error. Our opinion is based on the risks we identify at the time of the audit. Our overall audit opinion is based on 5 grades of opinion, as set out below.	
Opinion	**Assessment of internal control**
High Assurance	Overall, very good management of risk. An effective control environment appears to be in operation.
Substantial Assurance	Overall, good management of risk with few weaknesses identified. An effective control environment is in operation but there is scope for further improvement in the areas identified.
Reasonable Assurance	Overall, satisfactory management of risk with a number of weaknesses identified. An acceptable control environment is in operation but there are a number of improvements that could be made.
Limited Assurance	Overall, poor management of risk with significant control weaknesses in key areas and major improvements required before an effective control environment will be in operation.
No Assurance	Overall, there is a fundamental failure in control and risks are not being effectively managed. A number of key areas require substantial improvement to protect the system from error and abuse.

Priorities for Actions	
Priority 1	A fundamental system weakness, which presents unacceptable risk to the system objectives and requires urgent attention by management.
Priority 2	A significant system weakness, whose impact or frequency presents risks to the system objectives, which needs to be addressed by management.
Priority 3	The system objectives are not exposed to significant risk, but the issue merits attention by management.

Detailed Findings

Information Security checks Nov17 - consc