Information Security Checks 2018/19

City of York Council

Internal Audit Report

Business Unit: Corporate and Cross-Cutting
Responsible Officer: Corporate Director Customer and Corporate Services
Service Manager: Information Governance and Feedback Team Manager
Date Issued: 21 February 2019
Status: Final
Reference: 10260/026

	P1	P2	P3
Actions	**0**	**3**	**0**
Overall Audit Opinion	Reasonable Assurance		

Summary and Overall Conclusions

Introduction

1.1 In accordance with the agreed audit plan for 2018-19, information security checks were undertaken at West Offices in September 2018 and at Hazel Court in November 2018. The purpose of these checks is to assess the extent to which personal, sensitive and confidential data is stored securely and to ensure that data security is being given sufficient priority within council service areas.

1.2 Previous checks conducted in 2017-18 (November 2017) gave an overall opinion of Reasonable Assurance. It was found that there had been no discernible improvement from the position at the time of March 2017 checks with items containing personal, sensitive and confidential information still being left unsecured across both sites.

1.3 At the time of this audit (September 2018), the secure key storage system at West Offices had been in operation for almost a year and 30 teams were registered. The Hazel Court key storage system was installed in January 2018 and 20 keys had been allocated to teams at the time of this audit.

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 eleventh 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 had been left out overnight without appropriate security. Instances of information being left unsecured were recorded where these posed risks to the council, either because they contained 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 Annex 3.

Findings

West Offices

2.1 Overall, there was no improvement from the November 2017 checks. If anything, there has been a marginal decline in physical information security at West Offices, with almost twice as many items containing highly sensitive personal information being found

unsecured. However, it was at least encouraging to note that items were found in fewer service areas than in the previous checks. This was perhaps due to the fact that more areas are now using the secure key storage system.

2.2 It was observed that the vast majority of items found belonged to teams which had featured in the findings of the November 2017 checks, indicating that the required improvements to physical information security arrangements have not been made in these areas. Furthermore, it was disappointing to discover that almost one third of the items found belonged to teams that had registered with the secure key storage system. This would suggest that the system is not being used effectively, either due to it not being used consistently or, more likely, because not all items are being locked away before keys are returned to the key safe.

2.3 For these checks, all of the most serious data security breaches were found at West Offices and included:

- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

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 the office. These were through one or more cupboards in an area not being locked. A number of council assets were also left unsecured, including laptops, tablets, cameras and various keys (to other storage areas).

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. Particular attention should be paid to those rated as medium and high risk in the detailed findings in Annex 3.

Hazel Court

2.6 There was a significant improvement from the November 2017 checks. The vast majority of cupboards were locked and those that were not locked did not contain any personal data. There were also no instances of personal data being left out on work surfaces, either on desks or on top of cupboards.

2.7 Some work information (e.g. commercial job sheets and site inspection files) was left unsecured but this did not contain personal data and so represents only a very low risk to the council. xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

2.8 The previous checks observed that some of the storage facilities at Hazel Court were broken and that some teams were using open shelving as they did not have sufficient secure storage. New secure storage facilities have been purchased and installed in all office areas and the secure key cabinet system has been implemented.

2.9 There are plans to implement a secure key storage system for the work room, similar to that in operation for the office areas, which will also serve the purpose of ensuring only authorised drivers can access specific vehicle keys.

2.10 Findings from the Hazel Court information security checks are detailed in Annex 3.

Overall Conclusions

3.1 The council remains reasonably well protected against accidental disclosure of information. The majority of information is stored in cupboards. Cupboard doors are generally closed; the majority of cupboards are locked and the clear desk policy is largely adhered to throughout both offices.

3.2 However, despite the implementation of the secure key storage system at West Offices (which had been in operation for almost a year at the time of the information security checks), it appears more work is required to ensure that it delivers the intended information security benefits.

3.3 Following the previous audit, instruction was given to all teams to register with the secure key storage system. Not all teams have registered to date.

3.4 Items were also found in areas belonging to teams which had registered with secure key storage system. This would suggest that not all teams are making effective or consistent use of it. Teams that are already using the system should ensure that their procedures for locking cupboards at the end of each day are clear, understood and are followed.

3.5 Physical information security arrangements at Hazel Court are now much improved. This improvement is due to the provision of new storage facilities and secure key system but also indicates an improved culture within all teams in securing their information. Further improvements are planned which should see access to council vehicles better controlled.

3.6 Access to West Offices and Hazel Court buildings is controlled through perimeter security but at West Offices there is a risk of unauthorised access to information by individuals who legitimately have access to the building as a member of staff, a partner or a visiting member of the public.

3.7 There remain improvements to be made, particularly at West Offices, to protect against deliberate unauthorised access by ensuring all personal and sensitive information is locked away. Action is also required to ensure that confidential information (e.g. financial data) is kept securely.

3.8 It seems that not all areas of the council have sufficiently developed a culture and associated practice that recognises the importance of securing data and that all information held is an asset which needs to be protected.

3.9 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.

Agreed Action 1.1

A definitive list of all council teams/service areas will be compiled and used to record and administer the registration of teams/service areas with the secure key storage system.

A report will be presented to the Council Management Team (CMT) who will be requested to make a decision on whether or not it will be made a mandatory requirement for all council teams/service areas to register with the secure key storage system.

Priority	2
Responsible Officer	Facilities Manager & Information Governance Manager
Timescale	April 2019

Agreed Action 2.1

The detailed findings from these information security checks will be reported to the Governance, Risk and Assurance Group, CMT, Corporate Leadership Group (CLG) and Directorate Management Teams (DMTs).

Priority	2
Responsible Officer	Information Governance Manager
Timescale	April 2019

Agreed Action 3.1

Instructions on the use of the secure key storage system and on good physical information security management will be reviewed and updated. It will be ensured that the instructions make it clear that where lockable storage is broken or is inadequate that this is reported to Facilities Management immediately so that it can be rectified.

The revised instructions will be presented to CLG and to CMT and DMTs as part of the routine information governance updates. The instructions will then be re-issued to all staff via email and published on the intranet.

Priority	2
Responsible Officer	Facilities Manager & Information Governance Manager
Timescale	June 2019

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 Sep & Nov 18