Veritau
Assurance Services for the Public Sector

Information Security Checks 2019/20

City of York Council

Internal Audit Report

Business Unit: Corporate and Cross-Cutting
Responsible Officer: Interim Assistant Director – Legal and Governance
Service Manager: Information Governance and Feedback Team Manager
Date Issued: 24 October 2019
Status: Final
Reference: 10260/028

	P1	P2	P3
Actions	0	2	0
Overall Audit Opinion	Reasonable Assurance		

Summary and Overall Conclusions

Introduction

1.1 Information is one of the most valuable assets held by any organisation. Good information governance is a key element of delivering high quality services. A failure to secure personal and sensitive[1] data can lead to data breaches under the General Data Protection Regulation (GDPR) and Data Protection Act 2018. These breaches can cause significant reputational damage as well as the potential for financial penalties up to €20 million.

1.2 The council holds and uses large amounts of personal and sensitive data. Senior management recognise there are information governance risks associated with holding this information and that appropriate practices need to be followed by council staff.

1.3 In accordance with the agreed audit plan for 2019-20, information security checks were undertaken at West Offices and Hazel Court in August 2019. 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.

1.4 Previous checks conducted in 2018-19 (West Offices in September and Hazel Court in November 2018) gave an overall opinion of Reasonable Assurance.

1.5 At the time of this audit (August 2019), the secure key storage system at West Offices had been in operation for almost two years and 45 teams were registered as using the system. The Hazel Court key storage system was installed in January 2018 and all the teams within the building had been allocated a key to teams at the time of this audit.

Scope of the Audit

1.6 As part of this audit, the two main council offices, West Offices and Hazel Court, were visited. This was the twelfth 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] For example data defined as special category data under data protection legislation (such as race or religious beliefs) or other sensitive data such as commercially sensitive information.

1.7 The buildings were visited outside of standard working hours. 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 because they contained personal or confidential information. Instances of general security weaknesses were also recorded.

1.8 The findings are summarised below and detailed findings are set out in Annex 3.

Findings

West Offices

2.1 Access to the building is only permissible through the use of unique electronic key cards provided to each member of staff. The building also has round the clock security to prevent unauthorised access. However 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.

2.2 Overall, there was a modest improvement from the Autumn 2018 checks. We noted that there was a reduction in the amount of personal and sensitive data that was found in an unsecure location. This was particularly noticeable within the finance and safer york partnership service areas. However once again we found a number of documents containing personal data and assets within the housing team.

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

- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

2.4 As well as the most serious items noted above, there were a few 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.

2.5 A number of council assets were left unsecured, including laptops, tablets, phones, cameras and also a large number of keys for council owned properties with the address of the property attached to the keys and various other keys (e.g. to storage areas of council properties).

2.6 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

2.7 Access to Hazel court buildings is controlled through perimeter security, with a security officer located on the site at all times. Staff are required to keep all cupboards locked then place the keys in a key safe. The security officer on duty checks each night if any keys have not been returned and locks cupboards that have not been locked. A log is maintained of any instance of cupboards being left unlocked and any instances logged are then reported to relevant members of staff.

2.8 During our visit it was found that the vast majority of cupboards were locked and those that were not locked did not contain any personal data. There was one cabinet that we found to be unlocked which contained staff sickness/medical and interview records. There were a few instances of personal data being left out on work surfaces such as appointment cards and gas safety checks that contained customer names and addresses.

2.9 Some work information (e.g. road safety audit results) was left unsecured but this did not contain personal data and so represents only a very low risk to the council.

2.10 We also identified assets that were left in an unsecure location; these included mobile phone, tablets and keys for access to gas meters.

2.11 A new secure key storage system is being implemented in 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. While the new key storage system is being installed the vehicle keys are stored within a portakabin on site. At the time of our visit the portokabin was locked, the security officer provided us with access. Inside the portakbain the key safe used to store vehicle keys was unlocked and appeared to be broken.

2.12 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 around two years, at the time of the information security checks), it appears more work is required to ensure that it delivers the intended information security benefits. Guidance has been produced instructing all department line managers to arrange with security to use the secure key cabinet and this will be disseminated through directorate management teams.

3.3 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.

3.4 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

Guidance relating to the key tracker will be communicated to staff requiring all teams to use the key safe. Then escalate any service area that has not registered to use the key tracker to Corporate Management Team.

Priority	2
Responsible Officer	Total Facilities Manager
Timescale	31 March 2020

Agreed Action 2.1

Develop a process for monitoring and reporting when keys have not been returned to the key safe.

Priority	2
Responsible Officer	Total Facilities Manager
Timescale	31 March 2020

Annex 2

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.

Annex 3

Detailed Findings

Annex 3- Details of findings..xlsx

Where information resulting from audit work is made public or is provided to a third party by the client or by Veritau then this must be done on the understanding that any third party will rely on the information at its own risk. Veritau will not owe a duty of care or assume any responsibility towards anyone other than the client in relation to the information supplied. Equally, no third party may assert any rights or bring any claims against Veritau in connection with the information. Where information is provided to a named third party, the third party will keep the information confidential.