Veritau
Assurance Services for the Public Sector

Information Governance Compliance Check

Peak District National Park Authority

Internal Audit Report 2016/17

Business Unit: Corporate,
Responsible Officer: Interim Director of Corporate Strategy and Development
Service Manager: Interim Director of Corporate Strategy and Development
Date Issued: 08 March 2017
Status: Final
Reference: 69140/002

	P1	P2	P3
Actions	**0**	**1**	**1**
Overall Audit Opinion	Reasonable Assurance		

PEAK DISTRICT NATIONAL PARK

Summary and Overall Conclusions

Introduction

Information is one of the most valuable assets held by any organisation. Good information governance is increasingly accepted as a key element in delivering high quality services. A failure to secure personal and sensitive data and to manage key risk areas effectively can lead to data breaches under the Data Protection Act. These breaches can cause significant reputational damage as well as the potential for financial penalties up to £500,000. To date, the Information Commissioners Office has issued a number of fines to both public and private organisations who they have concluded have committed serious breaches of the Data Protection Act.

As part of the annual audit plan 2016/17, Internal Audit undertook a security sweep of Aldern House on Tuesday 10th January 2017.

Objectives and Scope of the Audit

The objective of the visit was to assess the extent to which data and assets were being held securely within Aldern House. This included hard copy personal and sensitive information as well as electronic items such as laptops and removable media. The audit was a review to ensure compliance with data security policies including a check of the clear desk policy. As this was the first check carried out it was requested that a relatively high level check should be undertaken and no searches of desk contents should be carried out.

Key Findings

Our information security compliance visit to Aldern House on 10th January 2017 found a number of unlocked pedestals and pedestals with the key in the lock. No sensitive documents were immediately obvious although we cannot be certain of the sensitivity as we were specifically asked not to undertake a detailed search.

We found a large volume of laptops and other equipment, including cameras, phones, monitors which had not been stored securely. There was a large collection of keys found inside unlocked key cupboards. We also found a substantial supply of stock and merchandise in an unlocked room. We have since been informed that a lock has been fitted to this room. This is a temporary store whilst Castleton Visitor Centre is being refurbished and the stock will be relocated back to Castleton w/c 10th April.

Overall Conclusions

It was found that the arrangements for managing risk were satisfactory with a number of weaknesses identified. An acceptable control environment is in operation but there are a number of improvements that could be made. Our overall opinion of the controls within the system at the time of the audit was that they provided **Reasonable Assurance**.

1 Security of Laptops and Equipment

Issue/Control Weakness	Risk
Some members of staff are not being security conscious and do not ensure that equipment is locked away after use or are securely locked to the desk.	The Authority is at risk of incurring data breaches, which may result in increased scrutiny from the ICO, possible monetary penalties and reputational damage. Assets not securely stored run the risk of being stolen.

Findings

Our review of offices found:

- A high number of unsecured laptops throughout offices
- Valuable equipment including cameras, video cameras, GPS, memory sticks, monitors, keyboards and PC towers that were unsecured.
- Open key safes which held a high volume of keys
- Money inside a collection envelope, and inside unlocked pedestals

Agreed Action 1.1

Key lockboxes contain many keys no longer used or required as sites have either been disposed of, or locks have been replaced. That said however, many keys are still in use and need to be better secured and so:

- The key safes will be kept locked at all times. Additional keys will be cut and will be kept on person.

These steps will be in place by the end of March 2017. In addition to this, further investigation will take place to source a new shared key safe. The aim is for this key safe to utilise existing access cards (restricted to appropriate staff) allowing audited access to certain groups of keys for certain staff. This is subject to a market evaluation which is to be completed by end of July 2017.

Regarding Pedestals, these only require locking if they contain sensitive information (such as personal or confidential material etc.). A reminder regarding this will be cascaded to staff as part of the communications regarding cameras and laptops etc. (see below)

Staff members have received a reminder regarding locking away equipment such as cameras and laptops when they are not in use. A further reminder regarding this will be cascaded to all staff. This will take place following some Operational Leadership Team

Priority	2
Responsible Officer	Interim Director of Corporate Strategy and Development
Timescale	Ongoing

briefings to take place by the end of July 2017.

The stock IT equipment is not currently locked away. These devices contain no data, and so pose little risk from a data loss point of view. The devices themselves are captured and recorded in an asset control database upon delivery. Access to the room itself is through doors secured with access control (at both ends of the corridor). Once the current ICT Infrastructure replacement project is complete, this stock equipment will be moved to be stored in the current server room (this will not contain server equipment following the replacement) and so will be locked behind a secure access control door with CCTV coverage in the room. This will be completed by the end of July 2017.

2 Information Security of Documents

Issue/Control Weakness	Risk
Some members of staff are not being security conscious ensuring that pedestals are locked which could contain sensitive information.	Sensitive and personal information is accessible and viewed by individuals who should not see the information. The Authority is at risk of incurring data security breaches, which may result in increased scrutiny from the ICO, possible monetary and reputational damage.

Findings

A number of unlocked pedestals and pedestals with the key in the lock were found throughout the building. No sensitive documents were immediately obvious although we cannot be certain of the sensitivity as we were specifically asked not to undertake a detailed search

Agreed Action 2.1

Not all pedestals require locking (particularly pertinent for those located at shared desks or hot desks etc.). A more in depth audit would be required to determine if any sensitive material could be found in unlocked pedestals. Access control doors prevent access to certain sections of Aldern House and so files are secure.

As a part of the agreed actions 1.1 above a reminder will be cascaded to staff regarding locking all pedestals that do contain sensitive information.

Priority	3
Responsible Officer	Interim Director of Corporate Strategy and Development
Timescale	Ongoing

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.

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.