Information Security Compliance Check

Peak District National Park Authority

Internal Audit Report 2019/20

Business Unit: Corporate
Responsible Officer: Director of Corporate Strategy and Development
Service Manager: Head of Information Management
Date Issued: 27 February 2020
Status: Final
Reference: 69140/008

	P1	P2	P3
Actions	**0**	**0**	**2**
Overall Audit Opinion	Substantial Assurance		

Summary and Overall Conclusions

Introduction

Information is one of the most valuable assets held by any organisation. Good information governance is 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 General Data Protection Regulations (GDPR), which became the primary Data Protection legislation on 25 May 2018 superseding the Data Protection Act. These breaches can cause significant reputational damage as well as the potential for financial penalties up to £17m (an increase from the £500k under the previous Data Protection Act).

As part of the annual audit plan 2019/20, Internal Audit undertook an information security compliance check at Aldern House on Wednesday 15th January 2020.

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.

Key Findings

Data and assets were seen to be largely held securely within Aldern House. The internal and external door locking system was in operation and cards were required to access all external and some internal doors. We were challenged by two members of staff while performing the compliance check. Both asked who we were and what we were doing. It is important that members of staff continue to be vigilant around the workplace. A new key safe had been installed in the Finance office to ensure pool car keys can be stored securely.

We found limited sensitive information left out on desks. A printed email detailing an employee's return to work details was the only document left out in the offices that contained potentially sensitive information. There was some non-sensitive documents left on desks. Maintaining clear desks overnight may help ensure sensitive documentation cannot be accessed inappropriately.

We saw a number of pedestals were unlocked or keys were left in the pedestal lock. It was agreed prior to the compliance check being performed that we would not investigate the contents in officer's personal pedestals. There may be a risk to the Authority if any of the accessible pedestals contained sensitive information and could be accessed by unauthorised members of staff.

The authority has a policy in place outlining that assets such as laptops should be securely stored overnight, but some unsecured laptops were identified. Laptops are encrypted and therefore do not pose a data security risk. A car key was found in an unlocked storage cabinet drawer with the number plate attached on a key ring. Large quantities of work wear was also stored in a room which did not require an access card to be accessed.

We found a confidential waste bin in one office that was not secure. The bin appeared to be defective, because we were able access documents whilst it was locked. This bin appeared to be different to others in use. This may result in unauthorised members of staff accessing confidential documents or documents containing sensitive information. Confidential waste bins should be locked securely and only accessible to people responsible for disposing of the waste. All other confidential waste bins that we checked were properly secured.

Overall Conclusions

The arrangements for managing risk were good with few weaknesses identified. An effective control environment is in operation, but there is scope for further improvement in the areas identified. Our overall opinion of the controls within the system at the time of the audit was that they provided Substantial Assurance.

1 Confidential Waste Bin

Issue/Control Weakness	Risk
A confidential waste bin did not have a securely locked lid.	Confidential documents or documents containing sensitive information can be accessed by unauthorised members of staff.

Findings

Confidential waste bins are used to securely store documentation with sensitive information prior to the documentation being destroyed. Confidential waste bins should only be accessible to the members of staff responsible for destroying and disposing of the waste.

The confidential waste bin in one office was not secure. The bin had a lock on it and this was locked. The key safe was also locked so the key could not be obtained. However, it was still possible to reach into the bin to retrieve documents although we did not examine the documents inside the bin. Other confidential waste bins that were checked were securely locked. This bin in this office is different to others used and appeared to either be defective or had not been closed correctly before being locked.

Confidential waste bins should not be accessible to unauthorised members of staff. They should be secure to ensure that the sensitive data contained cannot be accessed. This should help prevent a data breach from occurring that may cause monetary and reputational damage.

Agreed Action 1.1

The lock on this Confidential waste bin has been found to be broken, it will be repaired or replaced.

Priority	3
Responsible Officer	Director of Corporate Strategy and Development
Timescale	30 April 2020

2 Risk of theft

Issue/Control Weakness	Risk
Some assets are not secured overnight.	The Authority may have assets stolen.

Findings

The authority has a policy in place outlining that assets such as laptops should be securely stored or taken home overnight. However, some unsecured laptops were identified. Laptops are encrypted and therefore the risk of information being stolen is low but there is a risk to the Authority that physical property is stolen.

A car key was found in an unlocked drawer. The number plate was on an attached key ring. There is a risk that the car could be identified and stolen.

There was also a room containing a large amount of work wear. The room did not require a card for entry. The authority could be at risk of stock not being accounted for if the store is accessed by unauthorised persons.

Agreed Action 2.1

The users whose devices were found will be reminded about the policy.
A more general reminder about locking cupboards etc. will also be sent to all staff.

The current storage location is temporary, however this room will be locked to reduce the risk of losing stock. The clothing is administered by CBST, and so the key for this location will be held by this team, until such time that a more permanent stock storage location is found.

Priority	3
Responsible Officer	Director of Corporate Strategy and Development
Timescale	Reminders – 31 March 2020 Lock fitted – 30 April 2020

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.

PEAK DISTRICT NATIONAL PARK