Appendix 5

Information Security Compliance Check (January 2019)

Peak District National Park Authority

Internal Audit Report 2018/19

Business Unit: Corporate,
Responsible Officer: Director of Corporate Services
Service Manager: Head of Information Management
Date Issued: 26 April 2019
Status: Final
Reference: 69140/007

	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 2018/19, Internal Audit undertook a security sweep of Aldern House on Tuesday 15th January 2019.

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

Our information security compliance at Aldern House on Tuesday 15th January 2019 found a large improvement compared to previous visits. On the whole, all pedestals and cupboards were locked apart from those that did not contain personal/sensitive information. We found a small amount of unsecured personal documentation in the Customer and Business Support Team Office, such as volunteer expenses forms and a parking permit application in an in-tray.

In room 35 a key cabinet had been left open (key in lock) which contained approximately 16 keys including window, store cupboard and heritage toolbox.

Throughout the building we found a total of 3 laptops which had been left on desks unsecured. We were informed that laptops are encrypted and therefore would not pose a data security risk. However, it is PDNPA policy that staff should take home their laptops.

Overall Conclusions

It was found that 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 Information Security of Documents

Issue/Control Weakness	Risk
Some members of staff are not being security conscious and do not ensure that personal information is securely stored.	Personal information is accessible and viewed by individuals who should not see the information. The Authority is at risk of committing data security breaches, which may result in increased scrutiny from the ICO, possible monetary penalties and reputational damage.

Findings

Our visit found a small amount of unsecured personal documentation in the Customer and Business Support Team office. In a red in-tray we found five volunteer expenses forms which had name, address and car registration and a parking permit application which had name, address and phone number

In room 35 a key cabinet had been left open (key in lock) which contained approximately 16 keys including window, store cupboard and heritage toolbox.

Agreed Action 1.1

The in tray will be locked in the deputy manager's office at the end of each working day. Although the in-tray is cleared each day, some material is occasionally added by officers after CBST operating hours. We will trial this approach to see if it helps reduce the amount of paperwork that is left overnight. The risk here is mitigated by the CBST office being located within a secured part of the building, and the office being permanently manned during office hours (with no or minimal material then being left outside of business hours).

Officers have been reminded again not to leave keys in key cabinets.

Priority	3
Responsible Officer	Director of Corporate Services
Timescale	Immediate

2 Asset Security of Laptops

Issue/Control Weakness	Risk
Some members of staff are not being security conscious and are not abiding by Authority policy.	Assets not securely stored run the risk of being stolen, posing a risk to business continuity and also a financial risk in terms of loss of the asset and replacement.

Findings

Throughout the building we found a total of 3 laptops which had been left on desks unsecured:

- Room 58 asset 4586
- Mezzanine asset 3315
- Room 33 asset 3668

We were informed that laptops are encrypted and therefore would not pose a data security risk. However, it is PDNPA policy that staff should take home their laptops.

Agreed Action 2.1

The assigned users for these laptops have been reminded (or will be once they have returned from leave) about the policy for taking home or securing away laptops at the end of each day.

Priority	3
Responsible Officer	Director of Corporate Services
Timescale	Immediate

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