

**Yorkshire Dales National Park Authority**

**Draft Information Technology  
Systems Report**

**Year Ended 31 March 2008**

## **Contents**

- 1. Introduction and objectives**
  - 2. Detailed Findings**
  - 3. Statement of responsibilities**
- Appendix 1 – Action plan**

## **Page**

**3**  
**4**  
**6**  
**7**

## 1. Introduction and objectives

### Introduction and objectives

In accordance with our normal practice, we write to draw your attention to certain matters, which we identified during our review of general computer controls at Yorkshire Dales National Park Authority (YDNPA) which took place in November 2007. Our findings have resulted from performing tests of the high level design and implementation of key general computer controls only. We have not tested the operating effectiveness of general computer controls.

Our recommendations for improvement are summarised, together with the related management comments in the action plan in Appendix 1.

All findings and recommendations are made subject to the limitations set out on page 5.

We would like to thank Steve Funnell and his team for their assistance and co-operation during the audit.

## 2. Detailed Findings

<b>2.1 Logical security – SunSystems</b>	<p>During our review of password settings on the SunSystems, we noted that:</p> <ul style="list-style-type: none"><li>• Password length is set at 4 characters; and</li><li>• Only password length and expiry (30 days) are set. There is no setting for password history or account lockout.</li></ul> <p>Password lengths of five or less characters are more easily guessed or observed and therefore increase the risk of unauthorised access to systems. Even if passwords are forcibly changed, unless controls exist over password histories to limit password reuse, the effectiveness of the control is greatly reduced. Locking user accounts which fail repeatedly to login reduces the risk of a successful “brute force” password attack.</p>
<b>2.2 User account administration</b>	<p>During our review of user administration, we noted that:</p> <ul style="list-style-type: none"><li>• While there is a form widely available for the processing of leavers’ user accounts, this is not always effective in disabling accounts in a timely manner as the IT department is reliant on other staff to forward these forms; and</li><li>• There is no regular formal review of user accounts (Windows/SunSystems).</li></ul> <p>The absence of an effective leavers’ process increases the risk of unauthorised access through user accounts that remain active on the system once a user has left the organisation. Such accounts may be compromised by current employees or external intruders. This may compromise the availability, integrity or confidentiality of sensitive and/or confidential information.</p>
<b>2.3 Test of backups</b>	<p>During our review of back up processes, we noted that there is currently no formal procedure in place to test the readability of backup tapes.</p> <p>If backups are not readable, data may not be available for restoration when it is needed. This may lead to systems being unavailable or irrecoverable which may result in data loss.</p>

## 2. Detailed Findings (continued)

### 2.4 Environmental controls in the server room

During our review of physical security, we noted that with regard to the environmental controls in the server room:

- Temperature and humidity levels are not monitored;
- There is no fire detection or suppression control; and
- There are no flood prevention controls.

If appropriate environmental controls have not been implemented to adequately safeguard information resources, there is a risk that such resources may not be available when they are needed and/or recovery of such resources may be delayed in the event of an emergency. This may result in the failure of critical systems and the potential loss of financial data.

### 2.5 Software Licenses

During our review of software licensing processes, we noted that there are currently no periodic checks carried out to reconcile the software licenses implemented against those applications installed.

Lack of periodic reviews of the license inventory can lead to existence of unlicensed software on the computer systems which can expose the organisation to the risk of legal action for copyright infringement.

### 3. Statement of responsibilities

The Audit Commission published a 'Statement of responsibilities of auditors and of audited bodies' alongside the Code of Audit Practice. The purpose of this statement is to assist auditors and audited bodies by summarising where, in the context of the usual conduct of the audit, the different responsibilities of auditors and of the audited body begin and end, and what is expected of the audited body in certain areas. The statement also highlights the limits on what the auditor can reasonably be expected to do.

Our report has been prepared on the basis of, and our audit work carried out in accordance with the Code and the Statement of Responsibilities, copies of which have been provided to the Authority by the Audit Commission.

The audit may include the performance of national studies developed by the Audit Commission, where the auditors are required to follow the methodologies and use the comparative data provided by the Commission. Responsibilities for the adequacy and appropriateness of these methodologies and the data rest with the Audit Commission.

While our reports may include suggestions for improving accounting procedures, internal controls and other aspects of your business arising out of our audit, we emphasise that our consideration of Yorkshire Dales National Park Authority's system of internal financial control was conducted solely for the purpose of our audit having regard to our responsibilities under Auditing Standards and the Code of Audit Practice. We make these suggestions in the context of our audit but they do not in any way modify our audit opinion which relates to the financial statements as a whole. Equally, we would need to perform a more extensive study if you wanted us to make a comprehensive review for weaknesses in existing systems and present detailed recommendations to improve them.

It is the responsibility of audited bodies to maintain adequate and effective financial systems and to arrange for a system of internal controls over the financial systems. Auditors should evaluate significant financial systems and the associated internal controls and, in doing so, be alert to the possibility of fraud and irregularities.

Any conclusion, opinion or comments expressed herein are provided within the context of our opinion on the financial statements and our conclusion on value for money as a whole, which was expressed in our auditors' report.

We view this report as part of our service to you for use as senior management of Yorkshire Dales National Park Authority's for Corporate Governance purposes and it is to you alone that we owe a responsibility for its contents. We accept no duty, responsibility or liability to any other person as the report has not been prepared, and is not intended, for any other purpose. In the event that a third party asks to see this report, please ask for our consent before releasing it.

#### **Deloitte & Touche LLP**

Chartered Accountants

Newcastle upon Tyne

March 2008

For your convenience, this document has been made available to you in electronic format. Multiple copies and versions of this document may therefore exist in different media - in the case of any discrepancy the final signed hard copy should be regarded as definitive. Earlier versions are drafts for discussion and review purposes only.

## Appendix 1 – Action plan

Priority scale – H = High, M = Medium, L = Low

No.	Area	Recommendations	Priority	Management comments	Responsibility	By when
2.1	<b>Logical security – Sunsystems</b>	<p>Review the configuration of systems security on Sunsystems and enhance the system security as follows:</p> <ul style="list-style-type: none"> <li>- required password length should be increased (e.g. minimum of 8 characters);</li> <li>- a history of previous passwords should be retained (e.g. 10 previous passwords) ;</li> <li>- the lockout threshold should be set (e.g. 3 invalid login attempts).</li> </ul>	H			
2.2	<b>User account administration</b>	<p>Implement a formal process for processing leaver user accounts to include:</p> <ul style="list-style-type: none"> <li>- notification to IT from HR of all leavers/transfer either before or when they occur;</li> <li>- Regular reviews of active accounts (Windows and SunSystems) to verify whether all leavers' user accounts have been removed.</li> </ul>	H			

## Appendix 1 – Action plan (continued)

2.3	<b>Test of backups</b>	<p>Testing the on-going readability of backed up data on a regular basis.</p> <p>This will ensure that Yorkshire Dales National Park has the data available if data needs to be restored from backup tapes.</p>	M			
2.4	<b>Environmental controls in the server room</b>	<p>Perform a risk assessment of the physical security of the server room and give consideration to</p> <ul style="list-style-type: none"> <li>• installing measures to prevent water damage (e.g. raised flooring);</li> <li>• installing air conditioning to control humidity and temperature;</li> <li>• installing fire/smoke detectors in and around the computer room;</li> <li>• installing fire suppression equipment e.g. fire extinguishers, in or near to the computer room.</li> </ul>	L			
2.5	<b>Software Licenses</b>	<p>Formalise procedures for regular audits of software and include these in the information security policy. A rotation plan should be included in the audit plan to ensure that all PCs are covered in the audit. Such software audits should cover all platforms and local hard drives of all PCs.</p>	L			

# Deloitte.

Deloitte & Touche LLP is a limited liability partnership registered in England and Wales with registered number OC303675.

A list of members' names is available for inspection at Stonecutter Court, 1 Stonecutter Street, London EC4A 4TR, United Kingdom, the firm's principal place of business and registered office.

Tel: +44 (0) 20 7936 3000 Fax: +44 (0) 20 7583 1198.

Deloitte & Touche LLP is a member firm of Deloitte Touche Tohmatsu.

Deloitte Touche Tohmatsu is a Swiss Verein (association), and, as such, neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each member firm is a separate and independent legal entity operating under the names "Deloitte", "Deloitte & Touche", "Deloitte Touche Tohmatsu", or other, related names. The services described herein are provided by the member firms and not by the Deloitte Touche Tohmatsu Verein.

Deloitte & Touche LLP is authorised and regulated by the Financial Services Authority

Member of **Deloitte Touche Tohmatsu**