CAIRNGORMS NATIONAL PARK AUTHORITY

FOR INFORMATION

Title: **INFORMATION TECHNOLOGY CONTINGENCY PLANNING AND BUSINESS CONTINUITY**

Prepared by: **ANDY RINNING, BUSINESS SERVICES MANAGER**

Purpose

To provide the Audit Committee with an update on the current position on contingency planning for the Authority's Information Systems and risk assessment of the systems environment.

Recommendation

The Committee is asked to note the current position.

Executive Summary

Contingency planning for IT systems is about anticipating disastrous events and planning to cope with them should they arise. The IT environment for CNPA consists of an electronic link between Ballater and Grantown and between the Grantown offices, operating a range of administration applications for general office usage and internal and external email communications. The loss of IT and services can have a major impact where significant reliance is placed on this function. A draft business continuity plan has been prepared which sets out the action to be taken should circumstances arise where parts or all of the system should fail.

INFORMATION TECHNOLOGY CONTINGENCY PLANNING AND BUSINESS CONTINUITY – FOR INFORMATION

Background

1. As modern technology advances, businesses become ever more driven by and reliant on Information Technology to meet day to day business requirements. CNPA is no exception to this process.

2. The Park Authority inherited a fairly small system form the Cairngorms Partnership in 2003. The proposed scale and scope of functions to be carried out by the Park Authority resulted in significant investment in an IT system to meet the needs of the business for the first five years. This system has continued to develop as new business systems have been deployed within the organisation.

3. The current system consists of servers located in Grantown which provides general office functions and email facilities to staff across all premises. There is a dedicated private link between Grantown and Ballater which allows the planning staff direct online access to the shared drive facilities for normal business activities. It also allows the Ballater data to be downloaded overnight and backed up in the central server. In addition, there is a cable link to Morlich House connected directly to the central server for both IT and telephony functions.

4. Contingency planning is an essential function to ensure business continuity with a minimum of disruption. There are a number of business areas that can be classed as critical. These include Planning and Outdoor Access since both are statutory functions, have certain elements that are time driven and would be seriously disrupted in the event of failure. Other systems including accounts and payroll are equally at risk whilst the human resources system could function manually for a period of time without any serious implications.

Approach

5. For the most critical equipment there are maintenance or support contracts in place. The servers remain under warranty with the suppliers; the dedicated link between Ballater and Grantown is provided by British Telecom; and a support services contract in place to provide additional support to and cover for the IT Manager where the IT system is affected or there is a disruption in the services.

6. Data from the Grantown servers are backed up on a set programme of daily, weekly and monthly and kept off-site overnight. In the event of server failure, the latest data would be installed in any replacement server resulting in an almost current state, with up to a maximum of 24 hours lost data.

7. In addition to the servers located in Grantown, there is an additional server located in Ballater. In the event of this server failing, critical business functions can continue

to be carried out by staff relocating to Grantown until such times as repair or replacement has been carried out. Failure of the Grantown servers would mean loss of shared data and email facilities for such period of time as the server remained out of commission. In such circumstances the server in Ballater could be used in the interim to maintain business critical functions until the Grantown server is repaired or replaced. There is a possibility that all three servers could fail but the probability is highly unlikely. If such an event happened, a server would be purchased locally with sufficient capacity to provide business critical functions only until a replacement server was acquired.

8. The dedicated line between Ballater and Grantown is leased from British Telecom and allows the planning staff to have immediate online access to the central server shared data. It also allows Grantown staff to access planning data where required in the course of normal business functions. Failure of the line would mean loss of contact between the two offices resulting in no exchange of data and loss of backup of planning data. Planning staff would also lose access to email and the internet, which would seriously affect their business functions. In such circumstances members of the planning staff could relocate to Grantown to carry out critical functions until the line was reinstated. A local backup of data can be done and taken to Grantown for uploading onto the central server to maintain continuity.

9. Loss or corruption of currently installed financial or payroll software would result in a loss of data from the last backup point. In such circumstances software would be re-installed and the latest backup run to populate the data fields. The implications for staff would mean going back over the day's business to recreate the relevant transactions.

10. In relation to failure of PCs, printers or peripherals, one spare PC and printer is held in case required. PCs, printers and peripherals can however be purchased locally within a few hours in emergency situations. A number of staff are usually out of the office at any one time and staff can log on at any machine in any office thereby minimising the loss of time due to equipment failure.

Risk Analysis of Computer Environment

11. As part of the overall contingency planning exercise, a risk analysis of the CNPA computer environment was carried out and the results are shown in Annex A.

Forward Look

12. On a wider front, we are looking at the opportunities and benefits likely to be gained through the Scottish Executive's "On the Ground" initiative about collaborative sharing of backroom functions such as IT, HR and accommodation.

13. We are currently members of the Information Systems Group which draws representatives from a number of NDPBs, Agencies and the Scottish Executive looking at the advantages of sharing experience, systems, purchasing etc. As a

follow up to this we are exploring with SNH linking into their Wide Area Network which would provide us with a faster and better network plus additional support functions. We will also have an opportunity to participate in their contract for disaster recovery which would offer a secure means of resuming critical business functions within an agreed number of hours.

Conclusions

14. Whilst there are some critical business functions we are satisfied that our proposed contingency planning will ensure business continuity with the minimum of disruption.

15. In larger organisations, testing of contingency plans or individual departmental plans would be expected to be carried out annually to confirm business continuity. However, the CNPA system is fairly small and spread across three offices which allows a greater degree of flexibility to negate any failure in any one location. For that reason we do not consider full scale testing of the worst case scenario appropriate.

Recommendation

16. The Committee are asked to note the current position.

ANDY RINNING
14 August 2006

andyrinning@cairngorms.co.uk