CAIRNGORMS NATIONAL PARK AUTHORITY AUDIT & RISK COMMITTEE

FOR DECISION

Title: **CYBER RESILIENCE ACTION PLANNING**

Prepared by: **DAVID CAMERON, DIRECTOR OF CORPORATE SERVICES**

Purpose

This paper presents information to the Committee on work led by Scottish Government with all public sector bodies to implement a "Public Sector Action Plan on Cyber Resilience".

The paper seeks approval to proposed governance arrangements covering the Authority's work on Cyber Resilience.

Recommendations

The Audit & Risk Committee is asked to:

a) Approve the proposed governance arrangements to cover the Authority's work on Cyber Resilience set out in this paper.

Executive Summary

1. Following a number of high profile cyber-attacks on organisations in 2017, including a number of public sector organisations, the Scottish Government has launched a programme of work with all public bodies to implement a "Public Sector Action Plan on Cyber Resilience".

2. As an initial, preparatory action, all public bodies were requested to identify three key contacts for liaison with Scottish Government for this work going forward. For Cairngorms NPA, the following contacts have been confirmed:

    a) Strategic oversight: David Cameron, Director of Corporate Services
    b) Operational Management: Helen Rees, Governance and Information Manager
    c) Day to Day / Incident Response: Sandy Allan, IT Manager

3. Scottish Government is committed to working with partners to develop and disseminate a Cyber Resilience Framework by the end of June 2018 (Key Action 1 of the Action Plan).

Governance Arrangements

4. Key Action 2 of the plan requests that organisations establish clear governance arrangements for oversight of and delivery of Cyber Resilience Actions within each organisation.

5. For the Authority, and in line with existing governance arrangements, committee structures and recognised Non-Executive and Executive responsibilities, I propose that the governance arrangements should be:

   a) The Audit and Risk Committee takes responsibility for the strategic oversight and risk management of the Authority's Cyber Resilience Action Plans and Implementation. This identifies cyber resilience approaches as an identifiable element of the Committee's work, while allowing the Committee to ensure that such work is designed and implemented as an integral part of the Authority's internal control processes. For example, the Authority has already commissioned and reviewed and internal audit of IT and security processes which is directly linked to work on cyber security.

   b) The Audit and Risk Committee shall keep the full Board informed of its work in overseeing approaches to cyber security at least annually through its Annual Report to the Board and shall escalate matters immediately on exceptional basis should circumstances warrant.

   c) As the strategic link with overall responsibility for implementation of actions addressing cyber resilience, the Director of Corporate Services will support the Committee in its oversight and update on delivery of actions and implementation of the Cyber Security Framework, and in review of relevant policies and strategies.

   d) The Director of Corporate Services will lead the staff team involved in delivery of these actions and report as appropriate to the Authority's Management Team.

   e) The work of the Director of Corporate Services supports the Chief Executive, as Accountable Officer, is their personal responsibility for the security of the Authority's assets, including data assets.

6. I propose that Cyber Resilience is added as a standing agenda item for the Committee until further notice, in order that activities between Committee meetings can be reported and any Board level decisions sought.

David Cameron
24 January 2018
davidcameron@cairngorms.co.uk