WILTSHIRE COUNCIL

LOCAL PENSIONS BOARD
07 November 2024

Business Continuity and Cyber Security

Purpose of the Report

1. To provide our cyber security policy for consideration by the Board and recommendation to the Committee. The presentation will also include a summary on the Fund's Business Continuity Plan.

Background

2. Pension schemes hold large amounts of personal data and assets, which can make them targets for criminals. We need to take steps to protect our members and assets accordingly, which includes protecting them against 'cyber risk.

3. Cyber risk is complex, rapidly evolving and requires a dynamic response. Our assessment of risk, controls and response plans should be reviewed regularly. Normally, this means at least annually and more frequently if there are substantial changes to our scheme's operations.

4. The Pension Regulator's (tPR) General Code of Practice came into force on 28th March 2024. Cyber Security is a new area that was introduced as part of this Code highlighting the importance that tPR is committing to this area.

Business Continuity Plan

5. The Business Continuity Plan (appendix 1 of the meeting pack) provides a framework for a coordinated response to a business disruption.
6. The plan includes:
   - establishing key service information
   - detailing the activation process for the plan
   - identifying priority functions undertaken by the service and the resources and timescales associated with their recovery
   - outlining the incident management procedures and key staff
   - identifying alternative workplace locations
   - identifying and providing contact details for staff, suppliers and partners

7. Wiltshire Council's Emergency Planning Resilience & Response Team has rated our Business Continuity Plan as GOLD and acknowledged the time and effort put into our plan.

Cyber Security Policy

8. It is recognised that cyber risk is a real and growing threat, and the aim of the Cyber Security Policy (Appendix 2 of the meeting pack) is to set out how the Fund intends to assess and manage cyber risk.

9. The Fund aims to ensure that:
   - cyber risk is integrated into the overall risk management approach of the Fund.
   - all involved understand cyber risk and their responsibilities in helping to manage it.

- all data and asset flows relating to the Fund are identified to identify cyber risk.
- there is sufficient engagement on how those organisations are managing cyber risk.
- an incident response plan is maintained.

10. The Fund's approach to cyber governance is to follow the Seek, Shield, Solve and Review framework as summarised below:
    - Seek – understand and quantify the risk.
    - Shield – protect the funds and critical assets.
    - Solve – be able to react and recover quickly.
    - Review – check the effectiveness of our approach to cyber resilience.

11. The Fund will assess all advisers, providers and partner organisations identified by its Cyber Security Data Map (Appendix 2 of the meeting pack) to ensure they have appropriate arrangements in place to protect themselves against cyber threats, taking appropriate specialist advice as required. This will include assessing the Council as host for IT systems and services

Environmental Impact of the Proposal

12. Not applicable.

Financial Considerations & Risk Assessment

13. Not applicable

Legal Implications

14. There are no material legal implications from this report.

Safeguarding Considerations/Public Health Implications/Equalities Impact

15. There are no known implications at this time.

Proposals

16. The Board is asked to consider the cyber security policy for recommendation to the Committee.

Jennifer Devine
Head of Wiltshire Pension Fund

Report Author: Mark Briggs, Operations Manager

Unpublished documents relied upon in the production of this report: NONE