Wiltshire Pension Fund
Cyber Security Policy

Introduction

This document is the Cyber Security Policy of the Wiltshire Pension Fund ("the Fund"), part of the Local Government Pension Scheme ("LGPS"). It is recognised that cyber risk is a real and growing threat, and the aim of this policy is to set out how the Fund intends to assess and manage cyber risk.

Scope

This Cyber Security Policy applies to the Fund. The Fund is managed and administered by Wiltshire Council ("the Administering Authority") and whilst recognising that the Administering Authority uses its own services for ICT, it remains the responsibility of the Fund to assess the cyber security arrangements of both the internal arrangements and external arrangements.

Aims and objectives

In relation to cyber security, the Fund aims to ensure that:

- cyber risk management and cyber governance are integrated into the overall risk management approach of the Fund to reduce any potential loss, disruption or damage to scheme members, scheme employers or the Fund's data and/or assets.
- all those involved in the management of the Fund understand cyber risk and their responsibilities in helping to manage it.
- all data and asset flows relating to the Fund are identified and evaluated on a regular basis to identify the potential magnitude of cyber risk.
- there is sufficient engagement with advisers, providers, and partner organisations, including the Administering Authority, so that the Fund's expectations in relation to the management of cyber risk and cyber governance are clearly understood and assurance is gained on how those organisations are managing those risks.
- an incident response plan is maintained, and regularly tested, to ensure any incidents are dealt with promptly and appropriately with the necessary resources and expertise available.

Legislation and Guidance

The Fund is required to comply with the provisions of the Public Service Pensions Act 2013 and Pensions Act 2004 in relation to the establishment and operation of adequate internal controls to ensure the scheme is managed in accordance with the legal requirements. This includes data protection legislation which is particularly relevant in relation to the management of cyber risk.

Statement of Cyber Risk

The Fund holds and has responsibility for a large amount of personal data and financial assets which makes the Fund a potential target for cyber criminals. Some of the working of the Fund is outsourced to third party providers or provided by partner organisations. As a result, the Fund recognises that a substantial part of managing their cyber risk therefore means managing the cyber risk of these organisations. As well as deliberate cyber-attacks the Fund acknowledges that it is also exposed to accidental damage from cyber threats.

At a high level, the cyber risk to be concerned about is anything that damages the Fund, their members, or their employers because of the failure of IT systems and processes, including those of their providers and partner organisations. In practice, attention is focussed on several key areas:

- Theft or loss of member personal data
- Theft or loss of financial assets
- Loss of access to critical systems (e.g. the administration system)
- Reputational impact on the Fund, the Administering Authority, and employers
- Impact on members (e.g. the service members receive)

The Fund also recognises that, in addition to the direct effect of a cyber attack, there will be indirect effects such as the cost of rectifying any theft or loss of data or assets, meeting any regulatory fines or other financial settlement.

The Fund is aware that Information Security goes hand in hand with cyber security and as such the fund should take meaningful steps in protecting data held in other forms, such as in cabinets, paper form, SD cards etc.

This strategy sets out the Fund's approach to cyber governance. It includes how it intends to assess and minimise the risk of a cyber incident occurring as well as how they plan to recover should a cyber incident take place.

The Fund has researched the possibility of attaining cyber insurance to cover losses relating to damage to, or loss of information from, IT systems and networks but understands that the complexity around the requirements we would need in place, including those of our providers and partner organisations, means that obtaining such insurance would not be available.

Cyber Governance

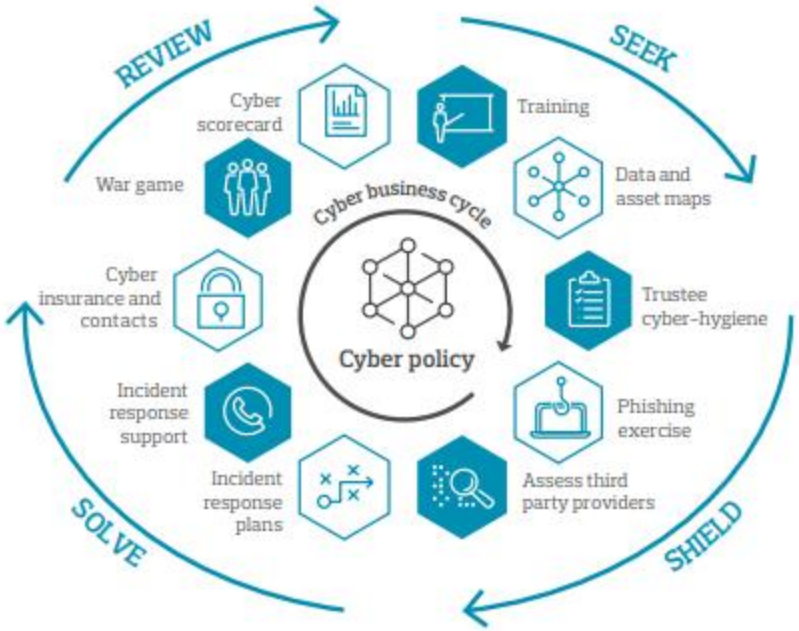
The Fund's approach to cyber governance is to follow the Seek, Shield, Solve and Review framework as summarised below:

Seek – understand and quantify the risk.

Shield – protect the Funds and their critical assets.

Solve – be able to react and recover quickly.

Review – check the effectiveness of their approach to cyber resilience.



The Fund's approaches in each of these areas is set out below:

Seek

Raise awareness, undertake training and assessment

Training:

- Pension Committee, Pension Board members and Fund Officers will receive regular training on cyber risk.
- The training may cover general cyber risk issues or explore a specific area of cyber risk.

Assessing Cyber Risk:

- The Fund will maintain a Data Map (an overview of where the Fund's data is held e.g. membership data and on what systems, for example with external managers, the Fund Actuary, etc.) that together document how the Fund's data flows between all the various stakeholders, advisers, providers, and partner organisations. This also categorises the frequency and materiality of these flows.
- This mapping supports a focused and proportionate approach to managing the risk of the data and asset flows with each stakeholder and external organisation.
- The Fund will undertake a high-level review of the Data Map every year, and as and when there is a change in supplier, or partner organisation. A more detailed review of the Data Map will be undertaken every three years.
- The Fund will seek regular assurance from the Administering Authority, in this instance acting as the ICT sponsor for a large part of the Fund's data (and from the key third party providers) that they assess and regularly review their attack surface to minimise the range of potential risks.
- The Fund will seek regular assurance from the Administering Authority (and from the key third party providers) that they regularly monitor any new threats which emerge and request that they advise the Fund when such threats are identified, including any steps to remedy these.

Risk Register

- Cyber risks are documented in the Fund's risk register, which is maintained by Fund Officers and updated on a quarterly basis. This information is considered as a regular item at Pension Committee and Pension Board meetings.

Shield

Set roles and responsibilities:

Responsible Officers

The Scheme Manager is the designated individuals for ensuring the cyber resilience framework outlined in this Policy is carried out for the Fund and ensuring they are satisfied with how cyber risk is being managed. The Scheme Manager is the Administering Authority and the responsibility has been delegated to the section 151 officer.

Oversight

The Pension Committee and Pension Board assists in ensuring the Fund meets its responsibilities and therefore will have oversight of this Policy.

Officers, advisers, providers, and partners

It is the responsibility of all Fund Officers to comply with this Policy. Fund providers and partner organisations will be made aware of this Policy and should provide regular reports on cyber risks and incidents.

Expectations of Pension Committee and Pension Board members and Fund Officers

Cyber Hygiene

Pension Committee and Pension Board members and Fund Officers are responsible for managing their own cyber risk and are encouraged to follow best practice in areas such as home working, use of personal email, password management and use of public networks.

Pension Committee and Pension Board members and Fund Officers are required to attend annual cyber security awareness training.

Pension Committee and Pension Board members and Fund Officers are required to confirm their adherence to this Policy on an annual basis and highlight any areas where adherence is not possible so that a secure alternative can be found.

Assessing advisers, providers, and partner organisations

The Fund will assess all advisers, providers and partner organisations identified by its Data Map 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.

The Fund will take a proportionate approach to assessing each organisation depending on the level of risk they pose to the Fund (as highlighted by the Data Map), with those advisers, providers or partner organisations that pose the greatest risk being assessed first and with more scrutiny.

The Fund will require regular reports from its advisers, providers and partner organisations on cyber risks and incidents.

The Fund will determine how regularly and to what extent further reviews are required, with those organisations that pose the greatest risk being reviewed more regularly.

Solve

Incident response planning

Incident response plan

The Fund's incident response plan will be developed in conjunction with our key advisers and providers, the Administration Authority, and cyber experts.

The Fund will inform all providers, advisers, and partner organisations of who needs to be notified when reporting a cyber incident.

Incident response support

The Administration Authority has cyber expertise to provide incident response support, including in relation to the Fund in the event of a cyber incident.

The Fund has agreed with the Administration Authority that in the event of a cyber incident affecting the Fund, they would also be supported by resources from the Council's ICT team to provide incident response support.

Incidents should be reported through the Administration Authority's Information Security and Cyber Security (sharepoint.com) site using the 'Report an Incident' facility.

Financial impact and insurance

The Fund will, from time to time, assess the possible financial impact of a cyber incident on the Fund recognising that in practice the impact is highly variable depending on the nature of the attack.

Review

Review of elements relating to this policy

As highlighted throughout, the approaches to managing cyber risk as outlined in this Policy will be reviewed on a regular basis, including thorough regular testing of the incident response plan, regular review of the Data Map, and regular assessments of providers and partner organisations cyber resilience.

Review of this policy

This version of the Cyber Strategy was reviewed and agreed by the Pension Committee and Pension Board on XXX. It will be formally reviewed, at least every three years or earlier if our approach to assessing and managing cyber risk merits reconsideration.

Wiltshire Council Administrator of Wiltshire Pension Fund

Wiltshire Pension Fund is administered by Wiltshire Council, as such Wiltshire Council have their own policies and procedures on cyber security and information security in which Wiltshire Pension Fund must abide by.

All staff have the responsibility to keep information safe and must follow the 3 principles of information security:

- Confidentiality – Only authorised personnel have access to the information. Protections in place 2FA, passwords, encryption, authentication, and defence on cyber security.
- Integrity – Information we have has to be accurate and used for the purpose it is intended for. Must not be altered accidently or maliciously.
- Availability – Information is accessible when needed by those who have the permissions to access such information.

More information on this Information Security and Cyber Security (sharepoint.com) and how staff can play their part: Play your part - and help to keep our information safe (sharepoint.com).

All staff must undergo yearly internal training in the following areas:

- Data protection
- Freedom of Information
- Records Management
- Information Security

Wiltshire Council policies can be found: Information Governance Policies and Templates (sharepoint.com)

References:

Pensions-Cyber-Risk.aspx (aon.com)

Information Security and Cyber Security (sharepoint.com)

Play your part - and help to keep our information safe (sharepoint.com)

Information Governance Policies and Templates (sharepoint.com)