Royal Borough of Kingston Pension Fund

Cyber Security Policy

(Approved by the Pension Panel- 21 September 2022)

THE ROYAL BOROUGH OF KINGSTON UPON THAMES

Pension Fund Cyber Security Policy

Introduction

This document is the Cyber Security Policy of the Royal Borough of Kingston Pension Fund ("the Fund"), part of the Local Government Pension Scheme ("LGPS") managed and administered by RB Kingston Council ("the Administering Authority"). The Administering Authority recognise that cyber risk is a real and growing threat and the aim of this policy is to set out how the Funds intend to assess and manage cyber risk.

Scope

This Cyber Security Policy applies to the RB Kingston Pension Fund as part of the shared pension service. Whilst recognising that the Administering Authority uses the shared services for ICT, it remains the responsibility of the Fund to assess the cyber security arrangements of both the internal arrangements and also external arrangements. The Fund is supported in this by rigorous audit processes and checks on an ongoing basis.

Aims and objectives

In relation to cyber security, the Fund's aim 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 or assets;
- all those involved in the management of the Fund understand cyber risks 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, the Royal Borough of Kingston, 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.

In setting this Policy, the Fund has had regard to the guidance from the Pensions Regulator, "Cyber security principles for pension schemes[1]", issued in April 2018[2], and ensured that the issues highlighted in that document are addressed by this Policy.

Statement of Cyber Risk

The Administering Authority for 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 as a result of the failure of IT systems and processes, including those of their advisers, providers and partner organisations. In practice, attention is focussed on a number of key areas:

[1] https://www.thepensionsregulator.gov.uk/en/document-library/regulatory-guidance/cyber-security-principles-the-pensions-regulator
[2] A new Code from TPR is expected to be laid in 2022, elevating the requirements for Cyber Controls to TPR Code see https://www.thepensionsregulator.gov.uk/en/document-library/consultations/new-code-of-practice.

- 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.

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.

Cyber Governance

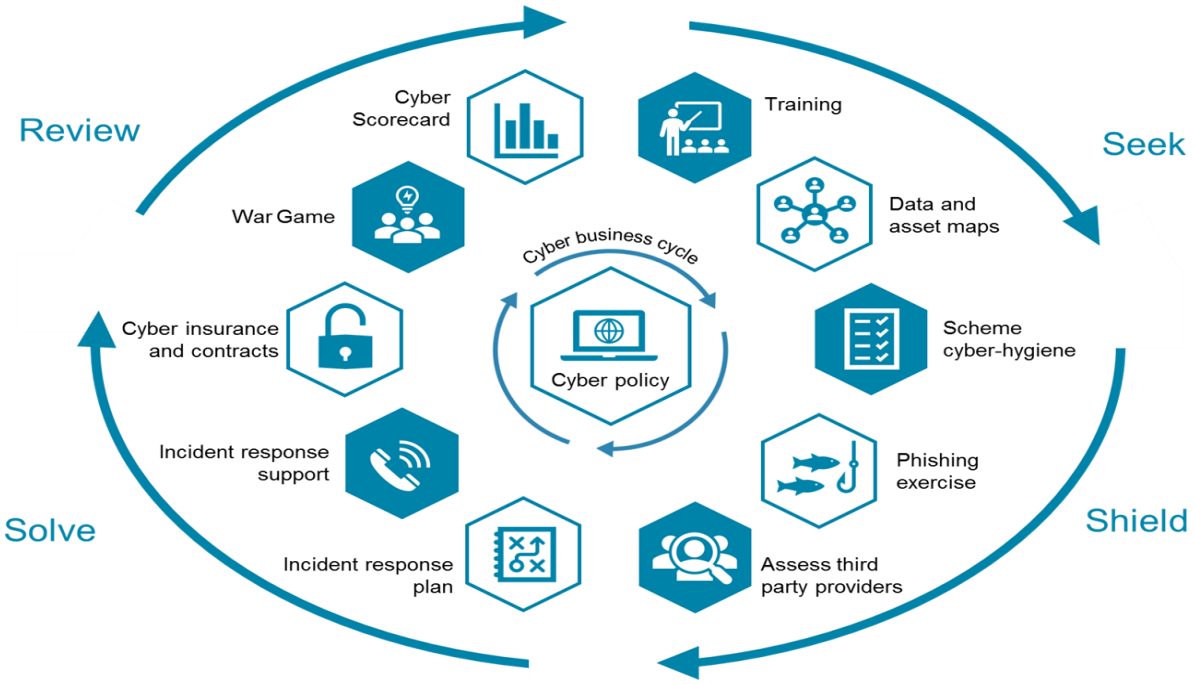
The Fund's approach to cyber governance is to follow the **Seek, Shield, Solve and Review framework** as summarised below:

A. **Seek** – understand and quantify the risk.

B. **Shield** – protect the Funds and their critical assets.

C. **Solve** – be able to react and recover quickly.

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



This is consistent with the framework adopted by the Council.

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

A. Seek

1. Raise awareness, undertake training and assessment

- **Training:**
  - Pension Fund Panel members, 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 – Data and Asset Mapping:**
  - The Fund will each maintain a Data Map and an Asset Map (this provides a overview of where the Fund's data is held e.g. membership data and on what systems along with an overview of where and on what systems the Fund's assets are held, for example with external managers, the Fund's custodian, London CIV etc.) that together document how the Fund's data and assets flow 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 and Asset Map every year, and as and when there is a change in adviser, supplier or partner organisation. A more detailed review of the Data and Asset Map will be undertaken every three years.
  - The Fund will seek regular assurance from the Council as Host Authority, in this instance acting as the IT sponsor for a large part of the Pension Fund's data (and from the key third party providers) that they assess and regularly review their attack surface in order to minimise the range of potential risks.
  - The Fund will seek regular assurance from the Council as Host 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 Panel and Pension Board meetings.

B. Shield

2. Set roles and responsibilities

- **Responsible Officers:** The Heads of Pensions Investment and Pensions Administration for the shared pension service are the designated individuals for ensuring the cyber resilience framework outlined in this Policy is carried out for the Fund.

- **Responsibility:** The Pension Fund Panel has been delegated ultimate responsibility for managing the Fund which therefore includes ensuring it is satisfied with how cyber risk is being managed.

- **Oversight**: The 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 advisers, providers and partner organisations will be made aware of this Policy and should provide regular reports on cyber risks and incidents. This includes working with the Host Authority to ensure the Fund's specific requirements are met.

3. Expectations of Pension Panel members, Pension Board members and Fund Officers

- **Cyber Hygiene:**

  - Officers and Councillors must follow the Council's Data Policies.

  - Pension Fund Panel members, Pension Board members and Fund Officers are responsible for managing their own cyber risk and even where they are not part of the Council's, are encouraged to follow the Council's Data Policies which the Funds have adopted as best practice in areas such as home working, use of personal email, password management and use of public networks.

  - Pension Fund Panel members, Pension Board members and Fund Officers are required to attend annual data awareness training provided by the Council.

  - Pension Fund Panel members, 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.

4. Assessing advisers, providers and partner organisations

- The Fund will assess all advisers, providers and partner organisations identified by its Data and Asset Maps 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 Authority 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 and Asset Maps), with those advisers, providers or partner organisations that pose the greatest risk being assessed first and with more scrutiny.
- The Fund will ensure all detailed assessments are carried out by those with relevant expertise.
- 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.

C. Solve

5. Incident response planning

- **Incident response plan**
  - The Fund's incident response plan will be developed in conjunction with our key advisers and providers, the Host 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 Host 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 Host 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.

6. Financial impact and insurance

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

D. Review

7. 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 through regular testing of the incident response plan, regular review of the Data and Asset Map, and regular assessments of advisers', providers' and partner organisations' cyber resilience.

8. Review of this policy

- This version of the Cyber Strategy was reviewed and agreed by the Pension Fund Panel on 21 September 2022. It will be formally reviewed, at least every three years or earlier if our approach to assessing and managing cyber risk merits reconsideration.

Further Information

If you require further information about anything in or related to this Policy, please contact:

rbkpensioninvestments@sutton.gov.uk