Worcestershire Pension Fund

Cyber Security Policy

Contents

Management summary

As a Fund we recognise that cyber risk is a real and growing threat, and risks can arise not only from the technology that we use itself, but also from the people using it and the processes supporting it. The aim of this policy is to set out how we as a Fund intend to assess and manage cyber risk, including understanding our cyber risk, the controls in place to manage cyber risk and how we intend to assess and minimize the risk of a cyber incident occurring, as well as how we plan to recover should a cyber incident take place.

The Fund has responsibility for a large amount of personal and financial assets which makes us a potential target to cyber criminals for:

- 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

As well as deliberate cyber-attacks the Fund acknowledges that it is also exposed to damage from cyber threats via our third-party providers by association, and this policy intends to take those third-party policies and their procedures in to account when determining the cyber risk. 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, loss of data or assets and meeting any regulatory fines or other financial settlement.

Background

The Pensions Regulator released initial guidance back in April 2018 on the issues it expects scheme managers to take into consideration to increase their cyber resilience. We are 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 General Code of Practice, "Cyber controls", issued in March 2024, and ensured that the issues highlighted and recommended as best practice in that document are addressed by this Policy.

- 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 and providers including the Administering Authority, Worcestershire County Council, 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.

Cyber Governance Policy Statement

The Pensions Regulator (TPR) recommends that schemes fully comply with The National Cyber Security Centre (NCSC) 10 steps to Cyber Security approach which is detailed below and broken down to reflect the Funds controls that are in place. The Fund is heavily reliant on the administering authorities' IT and Digital Service and as such, are restricted to the parameters set out by Worcestershire County Council in their Cyber Security Policy.

1. Risk Management

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.

2. Engagement & Training

All those involved in the management of the Fund understand cyber risks and their responsibilities in helping to manage it.

3. Asset Management

Majority of our cyber assets are held within our pensions database. All assets are recorded centrally and Heywood's have a published Asset Management Policy which details the lifecycle of an asset from onboarding through to secure disposal.

4. Architecture & Configuration

A secure-by-design approach means that our systems are difficult to breach, and architected such that should a breach occur, it is difficult for an attacker to traverse and navigate not only our internal Administering Authority systems but our pensions system as well. There are a number of protections that database hosts have in place including but not limited to, Distributed Denial of Service (DDoS) protection, Privileged Access Management and Multi Factor Authentication (MFA) as well as several authentication layers which are in place between the Administering Authority network and our pension records database.

5. Vulnerability Management

The Fund relies on the Administering Authority to provide the IT equipment and management of general software. The steps taken to mitigate any risks posed are set out in a number of their policies. The Administering Authority holds a valid PSN Compliance. Our external providers are minimal, and most do not have any direct access to our infrastructure. However, the Funds external pension system provider is an exception to this and complies with ISO 27001, ISO 9001, and Cyber Essentials Plus. Our provider also engages a cyber consultancy to undertake an annual independent review of their IT infrastructure. The latest review found no critical or high rated issues.

6. Identity & Access Management

The Administering Authority IT and Digital Service, and its Leadership Team, are responsible for maintaining the hardware and software components of the infrastructure the Fund relies on to access the pensions system. With access controls in place to only allow authorised users to access certain information systems with access being granted by IT and Digital Services directly upon authorised request. Our host provider adopts a similar approach with identity and access management being limited to authorised users.

7. Data Security

Whilst the Fund consults with the Administering Authority IT and Digital service, it remains the responsibility of the Fund to assess the cyber security arrangements of both the internal arrangements and external arrangements. The Fund is supported in this by the Administering Authority IT & Digital Service as well as rigorous audit processes and checks on an ongoing basis.

8. Logging & Monitoring

Logging and monitoring of core Administering Authority infrastructure is undertaken by the Administering Authority IT & Digital Service. Our pension system provider log and monitor their own issues within their vulnerability management tool and any vulnerabilities identified outside of the database are logged in a separate management tool.

9. Incident Management

An Information Security Incident Procedure is in place to help the Local Authority and managers assess the risks any incident presents and identify appropriate actions to take to mitigate the risks

and prevent the situation recurring. Our pension systems provider also holds a full Incident Management Policy and adopts a similar approach to incident management using a number of in house and external tools.

10. Supply Chain Security
Where a third party requires access to data derived from the Pension Scheme Database, or information classified as 'Official' or 'Sensitive', those users are subject to meet the same security requirements as the internal Council staff. These responsibilities must be laid down in the appropriate contract or Third-Party Access agreements.

Cyber Governance Approach

Considering the ten steps to Cyber Security, the Funds approach to Cyber Governance is to follow the six Pillars of Cyber Security, **Identification**, **Protection**, **Detection**, **Response**, **Recovery**, **Governance and Compliance** set out below, which is broadly consistent with the approach adopted by the Administering Authority and our pension system provider.

1. **Identification** - Understand and quantify the risk.
   - Catalogue and classify all digital assets (Hardware/Software/Data Repositories)
   - Ongoing Assessment of cyber risk (Itemised on the Risk Register)

2. **Protection** - Protect the Fund and critical assets.
   - Identify Clear Roles and Responsibilities only allow authorised users access.
   - Appoint Responsibility (Officers, Advisors, Providers and Partners)
   - Training – Specifically relating to Cyber awareness and how to report incidents.
   - Assess advisors and providers appropriately.

3. **Detection** – Preventative measures
   - Anomaly Detection: Spotting unusual patterns of behaviours that may signify a security incident.
   - Regularly review vulnerability management measures.

4. **Response** - Be able to react and recover quickly.
   - Incident Response Plan – a predefined strategy detailing handling and recovering from security incidents.
   - Incident Response Support – predefined roles to provide support in the event of an incident.
   - Business Continuity Plan – Including informing stakeholders and if applicable the public about the breach, it's implications and remediation.

5. **Recovery** – Restoring system functionality.
   - Backup and Recovery – ensuring regular backups to restore data integrity.
   - Improvements – logging lessons learned from incidents occurred to strengthen the fund's cyber security posture.

6. **Governance and Compliance** - Check the effectiveness of the Funds approach to cyber resilience.
   - Review Cyber Security Policies and Processes to ensure up to date compliance.
   - Review of how our data is transmitted (Data transmission grid)
   - Continuous evaluation of risks (Risk Register)

Further guidance for Schemes and Boards can be found at NCSC (National Cyber Security Centre) Cyber Security Toolkit for Boards - NCSC.GOV.UK

FOR OFFICE USE ONLY:

Worcestershire Pension Fund Breaches of Law Policy

Version: Final

Author: Emily Stanfield, Governance Lead
Dated: 04/06/2024

Signed off at: 25/06/2024