North East Scotland Pension Fund

nespf

Cyber Security Policy

February 2024

Contents

Document	**Cyber Security Policy**
Review Date	February 2024
Approval Date	N/A
Author & Team	M Suttie, Governance
Review Date	February 2025

Purpose Statement

This Cyber Security Policy has been prepared for North East Scotland Pension Fund, part of the Local Government Pension Scheme (LGPS), as administered by Aberdeen City Council.

Scheme Managers are required by law, under the Public Service Pensions Act 2013 and the Pensions Act 2004, to establish and operate adequate internal controls to ensure the scheme is operated in accordance with scheme rules and the law. Building and being able to demonstrate ongoing cyber resilience is one example of operating adequate internal controls.

The administering authority recognises that cyber risk is a growing threat. This policy 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 or assets. In addition to the direct effect of cyber attacks, there will also 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.

In preparing this policy, the Pension Fund has referred to guidance issued by the Pensions Regulator, the Pensions and Lifetime Savings Association (PLSA) and Aberdeen City Council (as the administering authority).

Application and Scope

1) What do we mean by cyber risk?

Cyber risk can be broadly defined as the risk of loss, disruption or damage to a scheme or its members as a result of the failure of its information technology systems and processes. It includes risk to information (data security) as well as assets, and both internal risks (e.g. from staff) and external risks (e.g. hacking).

<u>What are the direct consequences?</u>

These can include (but are not limited to):

- Payment disruption
- Identity theft
- Loss of members trust and reputational damage
- Financial loss
- Time cost
- Failure to meet regulatory obligations
- Fines issues by the Pensions Regulator

2) Who does this policy apply to?

Pension Funds hold large amounts of exploitable personal data and assets which can make them a target for fraudsters, scammers and cyber criminals. Therefore steps need to be taken to protect both members and assets against cyber risk.

Officers and Councillors must follow the Council's ICT policies, available at https://aberdeencitycouncilo365.sharepoint.com/sites/O365HUB/SitePages/ICS-Policies.aspx.

ACC's Information and Cyber Security Policy Framework is built on three corporate policies:

- ICT Acceptable Use Policy
- ICT Access Control Policy; and
- Protective Monitoring Policy

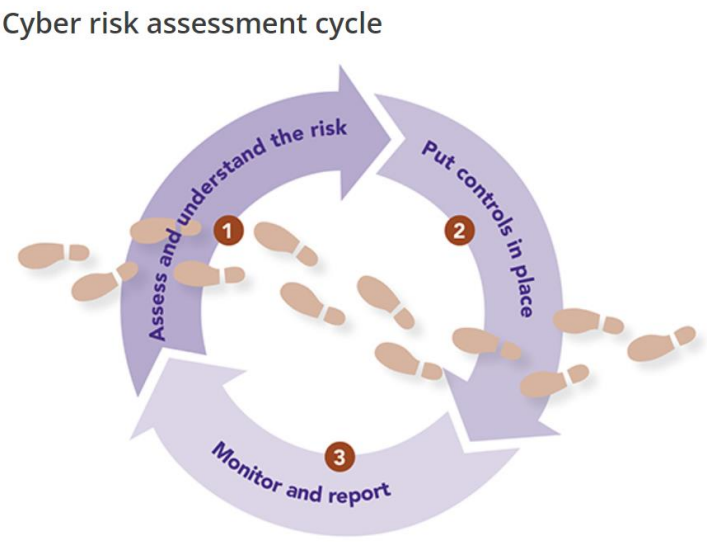
Most LGPS authorities are reliant on the administering authority for cyber security. This means that in the event of a major cyber attack the Fund will be competing for business continuity resources. Fund Officers as well as Pensions Committee and Board members must ensure, in their roles, they are satisfied the Pension Fund is adequately protected.

Funds also work with a wide range of external partners, providers and suppliers that handle their sensitive data including employers, AVC providers, software providers, actuaries, legal partners and custodians. The Fund recognises that a substantial part of managing our cyber risk means managing the cyber risk of these organisations. External agencies providing services to the North East Scotland Pension Fund are therefore required to provide assurances that they have identified cyber security risks, have in place arrangements to control and mitigate risks, and to report cyber security events to the Fund in a timely way.

External service providers include but are not limited to:

- Pension Software Provider (Heywood)
- Scheme Actuary (Mercer)
- Additional Voluntary Contribution Providers (Standard Life and Prudential)
- Global Custodian (HSBC)
- Auditors (Audit Scotland and Aberdeenshire Council)
- Legal Advisors (ACC, and external legal firms appointed through the City of Edinburgh Framework)
- Printing Companies (Adare)
- Overseas Payment Provider (Western Union)
- Tracing Bureaus (ATMOS, TUO and Target)

Risk Management



1. Assess and Understand

The Pension Fund should:

- Assess, at appropriate intervals, the vulnerability of a cyber incident of the Scheme's key functions, systems and assets (including data assets) and the vulnerability of service providers involved in the running of the Scheme.
- Consider accessing specialist skills and expertise to understand and manage the risk
- Ensure appropriate system controls are in place and are up to date (e.g. firewalls, anti-virus and anti-malware products)

In order to manage cyber risks, the Pension Fund will:

- Ensure critical systems and data are regularly backed up
- Maintain a cyber incident response plan in order to safely and swiftly resume operations
- Receive regular reports from staff and service providers on cyber risks and incidents

A robust cyber security risk management process will ensure that risks to essential services are identified, assessed, prioritised and managed in line with the Pension Fund's defined risk appetite (as set out in the NESPF Risk Management Policy). Effective risk management will allow decision-makers to make better, more informed decisions about cyber security.

Cyber risk is documented in the Fund's risk register which is maintained by the management team, updated on a quarterly basis and reported to the Pensions Committee and Board meetings.

Cyber risk also forms part of the wider Aberdeen City Council risk register which sets out their three lines of defence:

First Line of Defence (Do-ers)	Second Line of Defence (Helpers)	Third Line of Defence (Checkers)
• Trained and qualified staff • IT Security Technologies – devices to filter traffic and protect network, virus control software and domain access rules e.g. Conditional Access and Encryption • Operational procedures and guidance notes • Mandatory Information Governance Staff Training and IT Security Staff Training • Investigation into incidents and breaches • Monitoring & Alerting • Patch Management • System Change Management • Threat Hunting	• CMT Boards • Council Committees • D&T Senior Management Team (SMT) undertakes review of Cluster Operational Risk Register • Information Governance Group • ICT System Risk Assessments • Data Privacy Impact Assessments • Vendor Management • Policy documentation including, Information and Communication Technology (ICT) Acceptable Use Policy and ICT Access Control Policy, Protective Monitoring Policy • Annual review against Public Sector Cyber Security Framework	• External IT Health Checks for PSN Accreditation by Surecloud. Surecloud are National Cyber Security Centre and Check approved. • External Penetration testing on internet facing services by Surecloud. Surecloud are National Cyber Security Centre and Check approved.

Data Mapping

The Fund will maintain a Data Map and an Asset Map, providing an overview of where the Fund's data is held, and together these will document how the Fund's data and assets flow between all the various stakeholders, advisers and providers as well as detailing information on their respective data protection policies and procedures.

The Fund will undertake a high level review of the Data and Asset Map annually or as and when there is a change in adviser or supplier, and a full in depth review will be undertaken every 3 years or as required. The Data and Asset Maps will be the responsibility of the Systems Team.

2. Putting Controls in Place

- **Protect**

Training

Pension Committee members, Pension Board members and Fund Officers will receive regular training on cyber risk as part of their overall training plans.

Mandatory Information Governance training, covering data protection requirements under the UK General Data Protection Regulation (GDPR) and council information security requirements, is completed by all NESPF staff, with annual refresher training. Staff must also ensure they are familiar with the relevant ACC ICT and NESPF policies.

Contracts

Many of the Fund's contracts with external providers are historical in nature and therefore they may not make specific reference to cyber protection. Providers will recognise they have responsibilities in relation to cyber risk but are unlikely to provide open ended indemnification. It will be up to the Fund to ensure adequate protections are in place and that these are kept up to date with the changing environment.

Future contracts taken out with external agencies will consider how to have appropriate regard to cyber security risks in both the service specification and contract terms.

Data Transfer

The data mapping process should identify connections and the protect stage will ensure they are secured.

The Pension Fund has in place various policies in relation to the security of the data it handles and transfers including a Data Protection Policy, Breaches of Law Policy as well as internal procedures for 3rd party data requests, subject access requests, breaches of law and security incident reporting. In addition, a Systems Access Policy operates to ensure system access is controlled and monitored and password security is in line with ACC requirements.

Administering Authority

The Fund will seek regular assurance from the Council as the administering authority, that they assess and regularly review their controls and processes, that they monitor new threats which emerge and require that they advise the Fund when such threats are identified, including any steps to remedy these.

- **Respond**

Incident Response Plan

Our incident response plan has been developed in consultation with our key advisors, the administering authority and alongside our external providers.

In the event of a cyber incident the administering authority will support the Fund using the resources of its ICT team and the Fund will utilise their cyber expertise.

NESPF has its own Local Contingency Plan in place to respond specifically to critical incidents affecting its administration software provider, Heywood, to ensure pension payments can continue to be paid. The Fund's data is backed up daily following completion of daily processing. A full back up of the application software and the Fund's data is made weekly. A complete back up of all relevant systems is made monthly.

3. Monitor & Report

Cyber risk is monitored through the Fund's Risk Register. The Risk Register is reviewed quarterly by the senior management team and subsequently reported to the Pensions Committee and Board.

Protective monitoring will be undertaken by the administering authority of their digital and information assets with the goal of guaranteeing they have a suitable level of insight into how the ICT systems are being used.

Any incidents will be reported to the administering authority in accordance with their Information Security Reports Procedure i.e. through ServiceNow. Further guidance can be found in the NESPF Breaches Policy and accompanying procedure notes.

Supporting Procedures and Documentation

This policy is supported by wider NESPF and ACC governance policies and procedures, including but not limited to:

- Breaches Policy
- Communication Policy
- Risk Management Policy
- Systems Access Policy
- Data Protection Policy
- ACC ICT Acceptable Use Policy – key document
- ACC ICT Access Control Policy – key document
- ACC Protective Monitoring Policy
- Corporate Information Handbook
- ACC Information Security Incident Reporting Procedure

Responsibilities

Day to day responsibility for the implementation of this policy sits with the Chief Officer-Finance and dedicated staff within the Pensions Team.

The Pensions Committee will review this policy annually, or in the event of a policy revision and taking account of the results from any training needs analysis and emerging issues.

Any questions or feedback on this document should be forwarded to the **Governance Team**:

NESPF
Level 1, 2MSq
Marischal Square
Broad Street
Aberdeen
AB10 1LP

Email: governance@nespf.org.uk
Web: www.nespf.org.uk