National Federation of Voluntary Service Providers
Pension & Life Assurance Scheme

Information Security Policy

July 2026

Oranmore Business Park, Oranmore, Galway, Ireland, H91 TP2W
+ 353 (0)91 792316 pensionadmin@fedvol.ie www.fedvol.ie
Pension Authority No: PB67866 Revenue Approval No: SF7346

National Federation of Voluntary Service Providers Pension & Life Assurance Scheme

1. PURPOSE AND SCOPE:

The purpose of this Information Security Policy (the Policy) is to protect the confidentiality, integrity and availability of data, information and communications technology (ICT) assets, relating to the National Federation of Voluntary Service Providers Pension & Life Assurance Scheme (the Scheme). This Policy should be read in conjunction with the other components of the Scheme's Data Governance Framework.

The Policy and associated procedures are in place to achieve a high level of digital operational resilience and compliance with the Digital Operational Resilience Act (DORA) and to set out the Scheme's technical and organisational measures in compliance with Data Protection Legislation (The EU's General Data Protection Regulation and the Data Protection Act 2018).

The Trustees, while retaining overall responsibility for the Scheme's ICT risk management, are reliant on their service providers for pension and life assurance scheme services, including services that support critical or important business functions. The Trustees have set out their policy for managing service providers in the Operational Resilience Policy.

The Trustees management of ICT risk shall be implemented considering the principle of proportionality, taking into account:

- The nature, scale, complexity and importance of ICT-related dependencies.
- The risks arising from contractual arrangements on the use of ICT services concluded with ICT third-party service providers, considering the criticality or importance of the respective service, process or function, and the potential impact on the continuity and availability of financial services and activities.

2. SCOPE:

This Policy applies to all information assets owned or managed by the Scheme, including data, systems, networks, and facilities. It covers all Trustees, employers, contractors, and third-party service providers who have access to Scheme information assets.

3. INFORMATION SECURITY OBJECTIVES:

The Scheme's information security objectives are to:

- Protect the confidentiality of sensitive information.
- Maintain the integrity of data and systems.
- Ensure the availability of critical information and services.
- Comply with legal, regulatory, and contractual requirements.
- Maintain member confidence and trust.
- Support business continuity and operational resilience.

4. INFORMATION SECURITY MANAGEMENT:

The Trustees will achieve its information security objectives by ~~following~~ the following policies:

4.1. Information Security Principles:

The Trustees have adopted the following principles in relation to information security:

- Confidentiality – ensure Scheme data is only available to authorised individuals.
- Integrity – protect Scheme data from unauthorised alteration or tampering, ensuring it remains accurate and trustworthy.
- Availability – access to data, information and systems will be limited to what is necessary for each role, whether this is Trustee or Pension Scheme Manager.
- Accountability – assign clear responsibility for actions and decisions, with documented policies and audit trails.
- Risk management – vet, monitor and manage security risks posed by external providers e.g. National Federation of Voluntary Service Providers Supporting People with Intellectual Disability CLG, Irish Life (Registered Administrator and Investment Manager), Cornmarket, Grant Thornton and Align Advisory.
- Incident response – prepare, and test a plan to detect, respond to and recover from security incidents, including when reported by a third-party service provider.
- Awareness & training – Trustees and Pension Scheme Manager will receive appropriate training on information security.

4.2. Technical and organisational measures:

The Trustees' have developed technical and organisational measures to implement the principles of confidentiality, integrity and availability above. These are set out in Appendix 1 to this Policy.

4.3. Trustees use of own or employer devices:

Each Trustee must ensure the technical and organisational measures above are in place when they use their own devices for Scheme business. When they are using the devices of their employer, which will be subject to their employer's information security policy, then they must ensure that the controls are broadly similar to those in Appendix 1.

4.4. Risk Management:

Information security risks will be identified, assessed, and managed through a formal risk management process. This includes:

- Regular risk assessments to identify threats and vulnerabilities.
- Risk treatment plans to mitigate identified risks.
- Continuous monitoring of the risk environment.
- Regular review and update of risk assessments.

The Trustees recognise that the major risks for the Scheme relate to the information security stance of its third-party service providers. The management of this risk is set out in the Operational Resilience Policy. The Trustees will carry out the risk assessment on its own processes.

4.5. Roles and Responsibilities:

The Trustees are responsible for the overall implementation and oversight of the Policy.

5. INCIDENT MANAGEMENT:

An incident response plan will be put in place by the ICT third-party service providers to address and mitigate security breaches and confirmation of same will be provided to the Trustees on at least an annual basis. All ICT related incidents and significant cyber threats shall be recorded by the Trustees with appropriate procedures and processes in place to ensure a consistent monitoring, handling and follow-up of ICT related incidents. Given the Trustees' reliance on ICT third-party service providers, the Trustees will engage regularly with such providers in terms of incident management, including an agreed process for the notification of ICT related incidents in respect of the Scheme. In practice, this means the Trustees expect ICT incidents to be identified quickly, contained, reported, and learned from. Security incidents will be reported to the Pensions Authority in accordance with Article 19 of DORA.

6. ICT BUSINESS CONTINUITY:

To comply with Article 11(2) of DORA, the Trustees have updated the Operational Resilience Policy to incorporate ICT issues which is designed to:

- Ensure the continuity of the Trustee's critical or important functions.
- Quickly, appropriately and effectively respond to, and resolve, all ICT-related incidents in a way that limits damage and prioritises the resumption of activities and recovery actions.
- Activate, without delay, dedicated plans that enable containment measures, processes and technologies suited to each type of ICT-related incident and prevent further damage, as well as tailored response and recovery procedures established in accordance with Article 12 of DORA.
- Estimate preliminary impacts, damages and losses.
- Set out communication and crisis management actions that ensure that updated information is transmitted to all relevant parties in accordance with Article 14 of DORA, and report to the competent authorities in accordance with Article 19 of DORA.

Given the Trustees reliance on ICT third-party service providers, the Trustees will engage regularly with such providers in terms of their business continuity plans and effectiveness.

7. ICT TESTING:

A digital operational resilience testing programme (proportionate and risk-based) will be put in place. The programme will include a number of tests, including vulnerability assessments, gap analyses, as well as network security assessments. Critical ICT systems and applications will undergo yearly testing.

8. Legal Standing:

This Policy is not, nor is it intended to be, a legal document and is not intended to have legal effect or to be legally binding on the Trustee Board, nor to override the Trust Deed & Rules of the Scheme. The Trustees reserve the right at all times to depart from the terms of this Policy as it sees fit; for example, to accommodate a particular set of circumstances or a changing of views. Any departure will be exceptional, documented and approved by the Trustees.

9. Review and Revision:

This Policy will be reviewed annually and updated as appropriate to ensure its continued effectiveness, particularly in respect of the use of ICT services supporting critical or important functions by ICT third-party service providers. Any changes to the Policy will be communicated to all relevant stakeholders.

APPROVAL AND NEXT REVIEW DATE OF THIS POLICY:

This document was approved and came into effect as follows:

Document Control	
Approved By:	**Mr. James Skehan,** **Chairman and Professional Trustee,** **National Federation of Voluntary Service Providers' Pension & Life Assurance Scheme**
Approved By:	**Mr. John McHugo,** **Vice Chairman,** **National Federation of Voluntary Service Providers' Pension & Life Assurance Scheme**
Date approved:	**30th July, 2026**
Next review date	**July 2027**
Previous versions	**n/a**

Signed: _____ **Date: 30th July, 2026**

James Skehan,
Chairman & Professional Trustee.

Signed: _____ **Date: 30th July, 2026**

John McHugo,
Vice Chairman.

APPENDIX 1
– TECHNICAL AND ORGANISATION MEASURES

The Trustees have approved the following technical and organisational measures for use in information security

AREA	POLICY
Access Control	
Passwords:	• Enforce minimum 12-character passwords with complexity (uppercase, lowercase, numbers, symbols). • Require password changes every 90 days (or sooner for high-risk roles). • Ban password reuse (e.g., last 5 passwords). • Use multi-factor authentication (MFA) for all remote access, admin accounts, and third-party portals.
Role-Based Access Control (RBAC):	• Grant access based on job roles (e.g., Trustees, administrators, auditors). • Implement least privilege principle: Users only get access to data/systems necessary for their role.
Accounts:	• No shared accounts – each Trustee or Pension Scheme Manager must have individual accounts for all Scheme systems.
Access Reviews:	• Conduct quarterly access reviews to remove unnecessary permissions (e.g., for former trustees, employees?? or providers).
Session Timeouts:	• Automatically log out users after 30 minutes of inactivity.
Secure Remote Access:	• Use VPNs with MFA for remote access to internal systems. • Restrict VPN access to approved IP addresses (e.g., third-party provider offices).
Access Request/Approval Process:	• Require written approval from the Pension Scheme Manager or Trustees for new access requests.
Offboarding Procedures:	• Immediately revoke access for departing staff or providers. • Confirm revocation with the third party in writing.
Data Security	
Encryption:	• Encrypt the entire hard drive to protect data if the laptop is lost/stolen. • In transit: Use TLS 1.2+ for emails, file transfers, and web portals. • End-to-end encryption for communications with third parties (e.g., PGP for emails, SFTP for file transfers).
Data Masking/ Pseudonymisation:	• Mask sensitive fields (e.g., PPS numbers, bank details) in test environments or reports.
Secure File Sharing:	• Use password-protected, encrypted file-sharing platforms (e.g., Secure FTP, OneDrive with MFA, or dedicated pension industry portals). • Avoid unencrypted email attachments for confidential or restricted data.
Data Classification:	• Label data by sensitivity (e.g., Public, Internal, Confidential, Restricted). • Apply stricter controls to Restricted data (e.g., member medical or financial details).

AREA	POLICY
Data Retention & Disposal:	• Define retention periods (e.g., refer to the Retention Schedule in Data Retention Policy). • Use secure deletion methods (e.g., degaussing, certified destruction) for physical media
Screen lock:	• Lock screens after 5 minutes of inactivity.
Firewall:	• Enable a firewall to block unauthorized network access.
Anti-Malware:	• Install and update anti-malware software.
Automatic Updates:	• Keep the operating system and software up to date.
Secure Wi-Fi:	• Only connect to secure, trusted networks. • Prohibit use of public Wi-Fi for scheme-related work.
VPN for Remote Access:	• Use a VPN to access scheme systems or share sensitive data.
Remote Wipe:	• Enable remote wipe for lost/stolen devices.
Physical Security	
Secure Laptops:	• Use cable locks for laptops in shared spaces.
Clean Desk Policy:	• Prohibit leaving sensitive documents or devices unattended.
Visitor Controls:	• Require sign-in/sign-out and escort for visitors accessing scheme offices.