Security white paper

Nest Corporation public website

nestpensions.org.uk

Key document details

Owner:	Nest Information Security	**Version no.:**	5
Classification:	Public	**Date:**	January 2026

© 2026 National Employment Savings Trust Corporation. All rights reserved. Reproduction of all or any part of the content, use of the Nest trademarks and trade names is not allowed without the written permission of Nest. Nest does not warrant nor accept any responsibility for any loss caused as a result of any error, inaccuracy or incompleteness herein. This content is provided for information purposes only and should not be construed as financial, investment or professional advice or recommendation by Nest. Data may be obtained from third party weblinks, but these may not be error free and cannot be verified.

Introduction and purpose

This white paper considers the information security and data protection controls in place for the National Employment Savings Trust (Nest) Corporation with a focus on the controls for **nestpensions.org.uk** (hereafter known as the Pensions Website). This is where employers and members input their information in order to use our service.

The aim of this paper is:

- To give members and employers confidence that Nest handles any information input into the Pensions Website with appropriate care, considering security and data protection.
- To help organisations who have a requirement to evidence information security controls or provide information security assurance.

Overview of information security

Nest is a trust-based workplace pension scheme run by a Trustee, the Nest Corporation. The Trustee is comprised of up to 15 Board members and the employees of Nest Corporation.

As a public corporation, Nest Corporation reports to Parliament through the Secretary of State for Work and Pensions. Nest Corporation is an ISO 27001:2022 certified organisation and is compliant with the General Data Protection Regulation (UK GDPR) and the Data Protection Act (DPA) 2018 UK.

Nest has strict infrastructure, operational and security processes and procedures in place to safeguard all data and assets, not just because we have to, but it's the responsible and right thing to do for our customers.

Nest Information Security Management System (ISMS) meets IS27000:2022 standards and is independently certified by an officially recognised certification body on an annual basis. With all findings and areas needing improvement being put into our continuous improvement program, which is tracked on a quarterly basis by Nest Corporation's risk committee.

Nest upholds the principle of 'Data protection by design and by default' for its architecture and security posture. Information security is built into the development lifecycle of the Pensions Website and risks are continually assessed as part of system development and implementation through well-established quality control processes. These processes include running regular vulnerability scans and providing the documentation of build standards for different system components maintained by the IT teams as well as the Nest change management board signing off design and change implementation.

All the security controls and information technology that Nest deploys are independently tested by a CREST certified third party. This third party conduct annual testing of all relevant areas including the Pensions Website as well as external and internal IT infrastructure. The results of the testing feed into mature remediation processes and risk assessments for prioritisation.

In conclusion

Nest Corporation controls are designed to meet current data protection regulations and follow information security best practice to ensure personal information is protected.

If you have any specific questions on information security at Nest Corporation, please email us at:

information.security@nestcorporation.org.uk

Appendix 1: ISMS controls

1. Organisational Controls

Organisational controls cover governance, leadership, policies, assurance, risk management and oversight of information security at Nest.

Information Security Governance & Policies

Nest maintains a comprehensive suite of information security policies, standards and procedures aligned to ISO/IEC 27001:2022.
Policies are reviewed at least annually as part of continuous improvement and are approved by the Chief Risk Officer.

Risk Management

A mature risk management programme is in place, with each Nest Directorate maintaining its own Active Risks and Opportunities (ARO) register. All risks are captured within the ARO and assigned both a risk owner and an accountable executive. Each ARO register is updated and maintained by at least one risk and control business partner appointed by the accountable executive.

Security risk assessments are conducted for all changes, projects, suppliers, and technology components.

Documentation & Change Management

All operational processes and procedures are documented and made available to relevant personnel.
Design and change implementation follow formal governance, including technical review, quality checks, and signoff by the Change Management Board.

Supplier & Third-Party Management

Information security requirements are embedded within supplier contracts and service agreements.
Key suppliers are monitored to ensure they continue to meet Nest's security and data protection requirements.

Incident Management

An established incident management process ensures identification, reporting, investigation and resolution of security incidents and weaknesses.

Root cause analysis is performed, and trends are monitored and shared with the Executive Team.

Compliance & Assurance

Compliance with legal, regulatory, and contractual requirements—including UK GDPR and DPA 2018—is formally managed.
Technical compliance is maintained via vulnerability scanning, SIEM logging, and independent penetration testing by a CREST certified provider.
Nest undergoes annual ISO/IEC 27001 certification audits by an independent accredited body.

Business Continuity & Backup

Business continuity plans ensure that operations and critical information remain available within required recovery timeframes.
Backups are taken and tested regularly in accordance with approved backup policies.

Data Protection

Data protection controls ensure compliance with UK GDPR and DPA 2018.
Personal data processed for the Pensions Website is stored within UK/EEA data centres. A designated Data Protection Officer oversees adherence to regulatory requirements.

2. People Controls

People controls cover employee lifecycle, awareness, and security responsibilities.

Background Verification

All employees and contractors undergo background checks prior to employment.

Security Awareness & Training

Regular security and data protection training is provided to all personnel.
Content is refreshed to reflect emerging risks, tools, and Nest's operational environment.

Roles & Responsibilities

Roles include clearly defined information security responsibilities, reinforced through policy, training and ongoing assurance activities.
Principles such as least privilege, segregation of duties and accountable user behaviour are communicated and enforced.

3. Physical Controls

Physical controls protect Nest's people, premises, equipment, and information from unauthorised physical access or environmental hazards.

Secure Facilities

Physical security controls include defined perimeters, access restrictions, secure offices, reception controls, and monitored delivery or loading areas.

Clean Desk & Information Handling

A clear desk policy ensures sensitive information is not exposed when not in use.
Physical assets are securely stored, labelled and protected in accordance with classification requirements.

Information assets

Information assets are classified and handled in accordance with the Information Security Classification Scheme and the Information Handling Guidance.

4. Technological Controls

Technological controls protect information systems, networks, applications and data through secure configurations, technical safeguards, and monitoring.

Asset Management

An inventory of information and physical assets is maintained with assigned owners.
All information is classified, labelled and handled in line with policy.

Access Management

User access is granted based on role requirements and reviewed regularly.
Authentication, authorisation and monitoring ensure accountability.
Least privilege and segregation of duties are enforced throughout the environment.

Cryptographic Controls

Encryption is applied based on data sensitivity and system requirements.
Cryptographic key management follows defined procedures and industry best practice.

Operations Security

Systems are protected from malware through layered controls and continuous monitoring.
Logs are collected, correlated and analysed using a Security Information and Event Management (SIEM) platform.

Network & Communications Security

Networks are securely managed with appropriate technical controls.
A dedicated Security Operations Centre monitors for threats and responds to events.
Nondisclosure agreements apply to staff, suppliers, and third parties handling sensitive information.

Secure Development & System Maintenance

Security is integrated throughout the software development lifecycle.
Controls include secure coding guidelines, change control, system testing, security testing, environment segregation, and sanitisation of data used for development or testing.
Technical reviews are performed when platform changes occur.

Vulnerability & Patch Management

Regular vulnerability scanning and independent penetration testing are conducted.
Identified vulnerabilities follow a defined remediation process aligned with risk and impact.

Data protection

Data protection is ensured by having processes and controls in place that comply with the requirements of the UK General Data Protection Regulation (UK GDPR) and Data Protection Act (DPA) 2018. Nest has a dedicated Data Protection Officer who makes sure that all Nest activities are in line with UK GDPR and DPA requirements.

For more details on the locations where Nest processes personal data, please see our privacy policy.



Nest Corporation
10 South Colonnade
Canary Wharf
London, E14 4PU

nestpensions.org.uk

p144824 144800 2/2022