Risk and Compliance

Security white paper

Nest Corporation public website

nestpensions.org.uk

Key document details

Owner:	Nest Information Security	**Version no.:**	4
Classification:	Public	**Date:**	October 2024

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 27001:2017 certified organisation and is compliant with the General Data Protection Regulation (UK GDPR) and the Data Protection Act (DPA) 2018 UK.

Nest is working with external auditors to transition to ISO27001:2022 in order to be compliant with ISO27001:2022 before the October 2025 deadline.

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 IS27000:2017 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. See Appendix 1 for more information.

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

ISO 27K domain	Brief overview
Information security policies	The ISMS contains security policies, standards, procedures and guidelines to make sure information security at Nest is compliant to the ISO27001:2017 standard. These are reviewed and updated in a yearly cycle as part of Nest's continuous improvement commitment. Nest Corporation's information security policy is approved by the risk committee and distributed to all employees and key third parties.
Organisation of information security	Nest has a dedicated information security team who are tasked with protecting the confidentiality, integrity and availability of the information that Nest holds. Personal data for the Pensions Website is hosted within UK/EEA data centres. Please see our **privacy policy** for more detail. There is an established risk management programme in place with an associated risk register which is reviewed, updated monthly, and signed off by assigned risk owners.
Human resource security	All Nest employees and contractors are subject to background verification checks prior to employment. All personnel are given appropriate information security awareness, education and training which covers key information security topics, principles, and risks. All activities are updated regularly to ensure they are fit for purpose and meet Nest's current risk profile.
Asset management	Ownership and accountability of assets have been identified and cover the complete assets' lifecycle. All information and data within Nest are classified, labelled and handled to reflect the policy and guidelines in place. An inventory of assets associated with information and information processing facilities, which identifies each asset owner, is maintained.
Access control	Access to all information assets, applications and systems are defined based on the business role. Access controls include the ability to identify and authenticate all users together with the ability to monitor the actions of users to establish accountability. Access controls are regularly reviewed to ensure that they are still relevant and appropriate to the role being performed. Processes are in place to make sure that access is appropriate, for example, by conducting access reviews of key systems and data storage areas. Segregation of duties and least privilege are actively integrated into all ways of working, processes and procedures.
Cryptography	Cryptographic controls (encryption) are implemented at the appropriate level for the sensitivity of the information and system requiring protection. The cryptographic controls include a policy on the use of controls and the management of encryption keys.
Physical and environmental security	Controls are in place to protect Nest Corporation's sites, assets, systems and information from unauthorised physical access. These controls include a physical security perimeter, physical security controls, which provides secure offices, delivery and loading areas and a clear desk policy.
Operations security	Tools have been put in place which constantly work to detect, prevent and recover from malware. This is based on an agreed response plan to protect software and data from damage and to contain security incidents. All operating processes and procedures are documented, maintained and made available to relevant personnel and contractors if required for their job role.
Communications security	The combination of people, processes and technology being in place provides assurance that the transfer of information is appropriate, and the Network is securely managed. The network. Using a Security Information and Event Management (SIEM) tool, the Security Operations Centre (SOC) team monitor the network, log and respond to any network events found.

ISO 27K domain	Brief overview
	Non-disclosure agreements are in place as required for employees, third parties, vendors and suppliers. These are reviewed and updated as required.
System acquisition, development and maintenance	Security in development and support processes integrate: • the secure development policy, • the system change control procedures, • the technical review of applications after operating platform changes, • restrictions on changes to software packages, • security system engineering principles, • a secure development environment, • outsourced development, • system security testing, • system acceptance testing. Information used for development or testing is fully sanitised (in line with a defined best practice standard) before being used and its use is agreed with information owners in advance.
Supplier relationships	Information security in supplier relationships is addressed with contracts and supplier agreements which include appropriate information security statements. Key suppliers are monitored and reviewed to ensure they are delivering services in a way that meets our security requirements.
Information security incident management	Processes are in place to ensure investigation and reporting of information security incidents, events and weaknesses. Incidents and event trending are analysed, root causes are identified, and actions are taken to prevent recurrence or mitigate impact as part of a mature incident management process. Incident metrics are reported to the Executive team.
Business continuity management	Policies and plans are in place to maintain, restore operations, and to ensure availability of information at the required level and in the required time. These are tested on a defined basis. With backup copies of information, software and system images being taken and tested regularly in accordance with the agreed backup policy.
Compliance	Compliance with legal and regulatory requirements is achieved through identification of applicable requirements, intellectual property rights (IPR), protection of records, privacy and protection of personally identifiable information (PII) and regulation of cryptographic controls. Internal audits are completed on a yearly basis to make sure that Nest is meeting its legal and regulatory responsibilities. Technical compliance of the IT systems is ensured through automated vulnerability scans, ad-hoc vulnerability scans, SIEM log integration and penetration testing by an external CREST certified third party. Nest is audited annually for ISO27001 standard by an independent accredited certifying body.
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