Risk and Compliance

Security white paper

Nest Corporation public website

nestpensions.org.uk

Key document details

Owner:	Nest Information Security	**Version no.:**	1.0
Classification:	Public	**Date:**	July 2020

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 **nestpensions.org.uk** (hereafter known as the Pensions Website) controls. This is where employers and members input their information in order to use our service.

The two aims of this paper are:

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

Overview of information security

Nest Corporation is the Trustee of Nest established by legislation as a Public Corporation to run the Nest Pension Scheme. Nest Corporation reports to Parliament through the Secretary of State for Work and Pensions.

Nest Corporation is an ISO 27001:2013 certified organisation.

Nest Corporation is compliant with the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018.

Nest keeps members' assets and data safe as it's the responsible and right thing to do for our customers and also because of regulatory and legislative requirements. Strict infrastructure, operational and security processes and procedures are in place to safeguard all sensitive data and assets.

The Information Security Management System (ISMS) deployed at Nest is in line with ISO27000 standards. The ISMS is independently certified to the ISO 27001:2013 standard by an accredited certification body on an annual basis. Any findings or areas for improvement are fed into our continuous improvement cycle and tracked by Nest Corporation's risk committee on a quarterly basis. See Appendix 1 for more detail.

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 penetration 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 hopes that this white paper has given you the confidence that our security controls are designed to meet current data protection regulations and that Nest follows information security best practice to ensure your sensitive 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 ensure information security at Nest is compliant to the ISO27001:2013 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 is 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 and 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 ensure 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	Unauthorised physical access, damage and interference to Nest Corporation's sites, assets, systems and information are prevented and a clear desk policy is implemented. The secure areas include a physical security perimeter, physical security controls, secure offices, rooms and facilities and secure delivery and loading areas. Controls are implemented to protect against external and environmental threats.
Operations security	Operating processes and procedures are documented, maintained and made available to relevant personnel and contractors if required for their job role. Operations security have established mechanisms for the consistent deployment of technical counter measures for the detection of, prevention of and recovery from malware. This is based on an agreed response plan to protect software and data from damage from malware and to contain security incidents.
Communications security	Networks are securely managed with people, process and technology in place to provide assurance that the transfer of information is appropriate and managed. Segregation in the network environment is used as a control so that information cannot flow between

ISO 27K domain	Brief overview
	environments. The network is monitored with a Security Information and Event Management (SIEM) tool and by a Security Operations Centre (SOC) team working to log, monitor and respond to any network events. 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 secure development policy, 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, and 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 have been developed and implemented to maintain or restore operations and to ensure availability of information at the required level and in the required time. This is tested on a defined basis. Backup copies of information, software and system images are taken and tested regularly in accordance with an agreed backup policy.
Compliance	Compliance with legal and regulatory requirements is ensured 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 by the audit team on a yearly basis to ensure 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 meeting GDPR requirements and having process and controls in place that comply with the Data Protection Act (DPA) 2018. Nest has a dedicated Data Protection Officer who ensures that all Nest activities are in line with 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 4PZ

nestpensions.org.uk

p63006 60050 07/20