The New Homes Group takes the security of our customer and partner data very seriously.

Some of the main data security controls we use to manage corporate client data are as follows:

Risk Management

Our controls are aligned to the ISO/IEC27001/2 information systems security management standard. We review our controls against this framework regularly and are annually audited on these.

Information Security Policy and Governance

We have Information Security, Acceptable Use and Data Protection policies in place that are updated and distributed at least annually.
We have a team responsible for security, including an Information Security Officer and a Data Protection Officer.

Human Resource Security

Employees have security and non-disclosure clauses in their contracts, along with regular awareness communications.

Asset Management

All IT equipment including hard drives are disposed of using a data disposal solution that is approved to the UK Government's IMG IA Standard No. 5.

Access Controls

Complex passwords are mandatory to gain access to our network. Users are enforced to change these regularly.
An automatic system is in place to disable user accounts on the day that they leave employment.
Employees are provided with the minimum level of access required to perform their approved activities.
Administrator access rights are limited to essential staff and are reviewed regularly.

Encryption Controls

A Mobile Device Management (MDM) solution is in place and installed on all mobile devices to allow access to any company resources (email). Remote wipe is available in case a user loses their mobile device.
All laptops and mobile devices have full disk encryption in place.
Removable media is locked down on all devices, with access to write to removable media allowed for limited, approved users. Any data that is written is force encrypted.

Physical Security

Access to our main buildings, is controlled via swipe-card access.
Access to data centres is by approved request only and with limited, controlled personal having access rights.

Operations Security

We have an IT Support team and dedicated service desk with an incident response plan in place to deal with issues.
Anti-virus and anti-malware products are used across the group. Updates are distributed daily and monitoring is in place to detect any devices that fail to update. Users are unable to disable the Anti-Virus application, override the update schedule or change any of the enforced policies.
Updates to Windows and other software are managed centrally and tested before being applied in a timely manner. Critical patches are fast-tracked and where relevant are deployed within 7 working days.
We recognise the forensic and detective benefits provided by logging system activity. We use system logs to investigate incidents and to provide assurance over some of our automated processes.
Data from our systems is backed up daily, with application data backed up on an hourly schedule.
Remote Access and administrative access to network devices is managed and controlled using the TACACS+ protocol and integration with the users Windows logon credentials.

Network Security

The office network throughout the UK is connected by a dedicated secure Internal MPLS Network. Two data centres host our key applications.
Our breakout from the internal network to the internet is serviced by two pairs of firewalls. These are locked down to minimise the ports / IP addresses permitted for both inbound and outbound traffic.
A number of network monitoring tools are in place to monitor and manage network traffic. We have an Intrusion Detection and Prevention solution in place which is configured to block malicious network traffic.
The internal network is segregated from the internet using a DMZ network that is used to secure access to corporate systems & public facing websites.
We have segregated connectivity using separate protocols for both internal and external wireless networks. The internal wireless network can only be accessed using a company issued device and issued with the correct type of certificate.
We have a rolling schedule of Penetration Tests carried out by authorised external Testers to simulate attacks on both the internal and external infrastructure. We review and update our controls in response to findings after each test.

System Development and Maintenance

We have established development and change management processes that include segregation of duties.
Production data is anonymised to ensure development and testing is done on de-sensitised data.

Supplier Management

We have a supplier management framework that includes the provision of data agreements and questionnaires along with suitable contracts where appropriate.

Business Continuity

We have an organisational resilience policy and disaster recovery plans.
We conduct disaster recover tests and disaster scenario training annually.

Legal and Regulatory Compliance

We are subject to a programme of External Independent Audits.
We have reviewed our controls in line with the General Data Protection Regulation (GDPR) and have appropriate measures in place to meet the requirements.