Wates Information Security Statement

Reimagining places
for people to thrive.

Wates

Contents

Introduction

This document is intended to provide third parties a summary of Wates Group ('Wates') organisational and operational security controls. It is designed to deliver baseline information required for preliminary security assessments and due diligence conducted by third parties that are considering the engagement of Wates services.

Information Security Organisation

Formal responsibility for all aspects of Information Security outlined in this document, is assigned to our Group IT Director, and is operationally managed by our Head of IT Operations and Group IT Security Manager.

Wates Group Employees

All Wates employees are subject to pre-employment background screening to include prior employment, criminal, credit, professional, and academic references and where required, DBS checks. For employees working in enhanced security roles, Baseline Personnel Security Standard (BPSS) and Security Cleared (SC) clearances are required.

Wates colleagues are subject to ongoing security training in addition to organisational training courses which include GDPR, Corporate Responsibility, Diversity, and Inclusion and many more that align with an employee's job function.

Security Awareness

Security awareness training is part of the on-boarding process, and all colleagues are required to undertake this training on an annual basis. Security awareness e-Learning training is subject to regular review, to ensure training material remains current and topical.

Wates has a comprehensive programme including e-Learning training, multi-channel communications, including newsletters and corporate social media, as well as simulated phishing exercises designed to enhance our employees' awareness of common risks posed to the business.

Non-Disclosure / GDPR Due Diligence Agreements

Wates's business information may only be disclosed to third parties who are authorised to receive it, and only under the following conditions:

- The recipient is required to complete a non-disclosure and/or data-sharing agreement (if not subject to an existing contract).
- Where there is PII (Personally Identifiable Information) being shared, the relevant Data Protection Champion and where appropriate, a member of the Privacy/Legal Team have approved the distribution of information.

Risk Management

Risk assessments are conducted periodically and in accordance with Wates's risk appetite and ongoing business change.

Our Group IT Risk Management Programme is led by our IT Portfolio Team, reporting up to the IT Risk Committee which meets quarterly. The committee is comprised of IT senior leadership along with relevant stakeholders, such as Internal Audit.

Our risk register tracks all risks, and the IT Risk & Policy Manager performs quarterly reviews with the relevant control owners.

We operate multiple technical and procedural controls to identify and capture new and emerging risks to protect business information.

Regular assessments are conducted to:

- Define, assess, and manage information security risks to make sure that business objectives can be achieved.
- Manage security vulnerabilities according to their risk rating and ensure effective and proportionate controls are in place.
- Provide an organisational wide view of information security risks and their respective remediation plans.
- Ensure the appropriate resources are deployed to minimise all business and customer information risk with engagement of relevant stakeholders.
- Apply the requisite number of controls in a layered, effective way to reduce risk exposure.

Wates Group Policies

Wates has several policies, procedures and standards encompassing all aspects of Information Security. Each document has a dedicated owner and is controlled via our IT Portfolio Team which ensures document compliance. Our key policies and procedures include:

- Information Security Policy - based upon ISO 27001 Framework, this document provides practices for the establishment and maintenance of information security controls to protect Wates's information assets and stipulates responsibilities for all employees, third-party suppliers, and contractors.
- Security Incident Response Policy and Plans
- Acceptable Use Rules
- Access Control Policy
- Password Rules
- Business Continuity & Disaster Recovery Plans
- IT Risk Management Process and IT Risk Appetite Statement
- Change Management Procedures
- Supplier Management Process
- Software Patching Process

Identity & Access Management

- Wates operates a 'least privilege principle' when it comes to providing access to data.

- Access privileges may only be granted upon request of the appropriate line management and in line with an employee's job role.

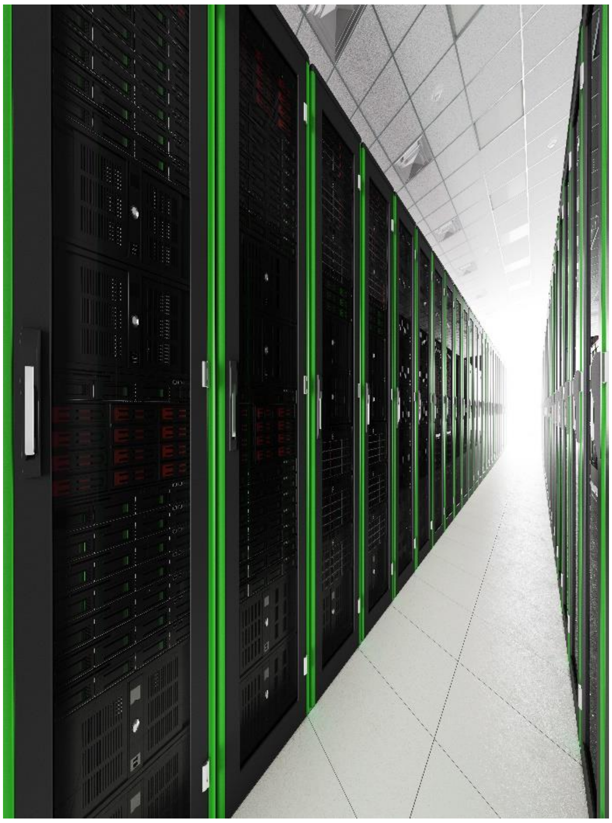
- External and internal audits are regularly performed to ensure access rights are appropriate and in compliance with policy.

- Infrastructure and business application teams are segregated to ensure incompatible provisioning of access is circumvented.

- Administrative and user access rights are reviewed on a quarterly basis.

- Remote access to Wates corporate network must use multi-factor authentication.

Physical Security



Physical security measures are implemented to ensure only authorised access to our Tier III facilities are in place.

We operate a combination of controls to restrict access to appropriate personnel only. These include, but are not limited to:

- Security fencing
- Security guards
- Physical barriers
- CCTV surveillance systems
- Biometric access controls
- Intruder alarms
- Secured data cabinets
- 3 Factor Authentication

Our data centres meet the following accreditations and standards:

ISO27001, ISO 14001, ISO 22301, ISO 50001, ISO 9001, Cyber Essentials Plus, PCI DSS / HM Government

Network Security

Wates uses numerous technologies and security controls across our networks to ensure our host environments and network traffic are secured effectively. Some of these technologies include:

- Intrusion Prevention and Detection systems
- 24/7/365 SOC and NOC monitoring
- Geo-blocking
- Managed firewalls
- Proxy servers
- VPN
- Conditional Access
- Multi-Factor Authentication (MFA)
- Single-Sign On (SSO)

Vulnerability Management / Penetration Testing

Leveraging best of breed vulnerability management technology from Tenable iO, we perform continuous monitoring of our host, internal and external network environments to ensure we have real-time visibility of any existing vulnerabilities.

Our platform combines vulnerability data, threat intelligence, data science and risk scoring, which enables us to quickly assess risk and prioritise any identified vulnerabilities and associated remediation activities.

Cloud based technology provides us with unified visibility and a continuous view of all Wates assets.

Additionally, we perform annual penetration testing of our environments by a third-party CREST approved provider.

As part of our commitment to securing our business and that of our customers and partners data, Wates holds the Cyber Essentials Plus accreditation for our whole organisation.

CYBER
ESSENTIALS
CERTIFIED
PLUS

End-User Device Security

As we have an extremely mobile workforce, ensuring the security of our end-user devices is of paramount importance.

All Wates workstations and laptops have the following installed:

- Endpoint Detection and Response protection including anti-virus/anti-malware software
- Pre-configured ‘standard build’ image
- USB ports blocked
- Laptops are encrypted with Bitlocker AES256 bit encryption
- Local administrative rights disabled
- Mobile Device Management (MDM) for tablets and smartphones (password protection policies, software management and remote wiping)
- Multi-factor Authentication (MFA)

Threat Management

Wates managed security provides threat intelligence across our company. A multitude of security solutions and threat hunting techniques, some of which are proprietary - provide us with the business intelligence to know what is dominating cyber security, as well as any nefarious activity that may specifically wish to target us.

Services include:

- Deception Technologies (Honeypot, threat receivers, honey tokens)
- Malware mitigation (global malware DB)
- SOAR/SIEM threat analytics
- Threat detector
- Full network traffic capture & deep packet analysis
- Suspicious access attempts
- Credential and data leakage monitoring

Patch Management

Vendor supplied software used in production systems must be maintained at a level supported by the vendor/supplier.

- Operating System security updates are reviewed and applied as appropriate to servers every month.
- Applications are regularly checked for available updates.
- Workstations are updated from Microsoft automatically.
- All critical and high vulnerability patches are applied within two weeks.
- All updates are subject to formal change management procedures.

Security Incident Management

Wates operates a robust Security Incident Management Policy and Plan, which ensures incidents are managed efficiently and thoroughly, with minimal impact to business operations.

Key aspects of our capabilities include:

- Effective communication and timely notification to all appropriate stakeholders and personnel when an incident happens
- Potential security incidents responded to promptly
- Any incident is investigated efficiently and thoroughly
- Identification and mitigation of any risks associated with an incident
- Annual incident response workshop
- 24/7/365 response team
- Managed Security Services Partner accredited for FIRST & CREST, CBEST, CBEST, CSIR and NCSC approved CHECK services

- SIRT Activities:
  - Malware analysis and detonation
  - Forensic analysis
  - Threat intelligence
  - Data mining and searches
  - Containment strategies

Vendor Security Management

Our IT Portfolio Team governs the IT Risk Management Process and manages the IT Supplier Management Process, which ensures that we can identify and manage all potential risks associated with third party vendors, which includes risks to information security.

All new vendors are subject to stringent due diligence reviews and security assessment as part of the RFI/RFP and project management processes.

Third parties with access to Wates's business information are subject to the requisite GDPR data sharing agreements and/or appropriate security clauses which are included in the Terms and Conditions of any contract.

Regular service reviews are performed with all contracted vendors to ensure compliance to any security requirements are maintained.

Governance and Compliance

IT Security in conjunction with the Infrastructure, Business Applications and Privacy Team regularly review our systems, policies, and procedures, which are guided by best practice methodologies and frameworks such as ITIL, ISO 27001, Cyber Essentials Plus, HMG Security Policy Framework, NCSC, and CIS.

External audits are performed on an annual basis which reviews key IT controls associated with our financial systems.

Internal audits are periodically performed in support of our organisational risk assessment and Group Board objectives and include Information and Cyber Security.

For more information contact: Danielle Hamilton, Wates IT Security Manager
danielle.hamilton@wates.co.uk

September 2024