

R&M POLICY · DATA AND CYBER SECURITY

Cyber Security Policy

R&M Property Group Ltd

Document	RM-DC-02
Version	1.0
Issued	24 June 2026
Approved by	Thom McKenna, Director
Website issue	22 October 2026

1. Purpose and Policy Statement

R&M Property Group Ltd and KWIKHAUS () are committed to protecting the confidentiality, integrity, and availability of all information assets, digital systems, and data under our control. As a developer operating within public sector frameworks we recognise that our cyber security responsibilities extend beyond the protection of our own commercial data to encompass the safeguarding of sensitive information belonging to Client Organisations, development partners, and the communities we serve.

This policy establishes the principles, responsibilities, and controls that govern cyber security across all R&M operations. It applies to all company systems, devices, data, and networks, and to all individuals who access them. The policy is designed to ensure that R&M maintains robust defences against the evolving cyber threat landscape, that we meet our obligations under applicable legislation and regulatory frameworks, and that our Client Organisations can have full confidence in the security of information shared with us through partnership arrangements, development agreements, and framework call-off contracts.

R&M is committed to continuous improvement in cyber security maturity. We currently hold Cyber Essentials certification, demonstrating that we have implemented the fundamental technical controls recommended by the National Cyber Security Centre (NCSC) to protect against the most common cyber-attacks. We are committed to achieving Cyber Essentials Plus certification - which includes independent, hands-on technical verification of our controls - by October 2027. This commitment reflects our recognition that working with public sector Client Organisations on sensitive development projects demands the highest standards of cyber security assurance.

2. Scope and Application

This policy applies to:

- All directors, managers, and employees of R&M Property Group Ltd and KWIKHAUS
- All subcontractors, agency workers, consultants, and professional advisors who access R&M systems or data
- All supply chain partners who handle, process, or store data on R&M's behalf or in connection with R&M projects
- All IT systems, hardware, software, cloud services, mobile devices, and removable media owned or used by R&M
- All data processed, stored, or transmitted by R&M, including personal data, commercial data, project data, and Client Organisation data
- All R&M offices, construction sites, and any remote or mobile working locations
- All projects delivered through public sector procurement frameworks

The policy is communicated to all employees at induction and forms part of the employment terms. Supply chain partners and consultants are required to acknowledge the policy as a condition of engagement on R&M projects.

3. Legal and Regulatory Framework

This policy supports R&M's compliance with the following legislation, regulations, and standards:

- UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 - governing the processing and protection of personal data, including data belonging to employees, Client Organisation personnel, residents, and members of the public
- Computer Misuse Act 1990 - prohibiting unauthorised access to computer systems and data
- Network and Information Systems Regulations 2018 (NIS Regulations) - establishing security requirements for network and information systems across essential services and digital service providers
- Privacy and Electronic Communications Regulations 2003 (PECR) - governing electronic communications and direct marketing
- Cyber Essentials Scheme - the UK Government-backed, NCSC-supported certification scheme that sets out baseline technical controls for cyber security
- NCSC Guidance - including the 10 Steps to Cyber Security, Small Business Guide, and sector-specific advisories published by the National Cyber Security Centre
- PPN 09/14 - Government Procurement Policy Note on cyber security in public procurement, requiring suppliers to government contracts to demonstrate appropriate cyber security measures

R&M also has regard to ISO 27001 principles for information security management when developing and reviewing its cyber security controls, and is committed to aligning with the NCSC's Cyber Assessment Framework where relevant to public sector framework delivery.

4. Cyber Essentials Certification and Roadmap

Current Certification: Cyber Essentials

R&M Property Group Ltd currently holds Cyber Essentials certification. This certification, administered under the NCSC's Cyber Essentials scheme, confirms that R&M has implemented the five fundamental technical controls that protect against the most common internet-based cyber attacks:

- Firewalls and internet gateways - boundary controls are in place to manage and restrict inbound and outbound network traffic, preventing unauthorised access to internal systems
- Secure configuration - all devices and software are configured to reduce vulnerabilities, with unnecessary services, accounts, and default credentials removed or disabled
- User access control - access to systems and data is restricted to authorised individuals on the principle of least privilege, with unique user accounts and appropriate access permissions
- Malware protection - anti-malware software is installed and maintained on all devices, with real-time scanning and regular updates to detect and prevent malicious software
- Patch management - operating systems, applications, and firmware are kept up to date with security patches applied within fourteen days of release for critical and high-risk vulnerabilities

Certification is renewed annually through self-assessment and independent verification by an accredited Cyber Essentials certification body. Our current certificate is maintained and available for inspection by Client Organisations and the Framework Manager on request.

Commitment: Cyber Essentials Plus

We commit to achieving Cyber Essentials Plus certification by October 2027. Cyber Essentials Plus builds on the baseline Cyber Essentials controls by adding independent, hands-on technical testing of the organisation's systems. This includes vulnerability scanning of internet-facing infrastructure, simulated phishing exercises, and verification that security patches and malware protections are functioning as declared. Achieving Cyber Essentials Plus will provide Client Organisations with independently verified assurance that R&M's cyber security controls are not only documented but are actively effective in practice.

Ian Skates, Financial Director, is responsible for budgeting for the Cyber Essentials Plus assessment and any remediation works required. Phillip Hollingworth, Compliance Officer at Spectra Safety, is responsible for coordinating the assessment process and ensuring readiness. The target date for achieving Cyber Essentials Plus is no later than October 2027.

5. Roles and Responsibilities

Directors

Thom McKenna (Director) has overall accountability for cyber security and for ensuring that this policy is implemented, resourced, and reviewed. Jon Scour (Operational Director) is responsible for ensuring that cyber security controls are applied consistently across all active construction sites and operational activities. Ian Skates (Financial Director) is responsible for ensuring that adequate budget is allocated to cyber security measures, including certification, training, and technology investment.

Compliance Officer

Phillip Hollingworth, Spectra Safety serves as R&M's designated Compliance Officer with responsibility for cyber security governance. Phillip is responsible for maintaining this policy, coordinating Cyber Essentials certification and renewal, managing the cyber incident response process, overseeing cyber security training, monitoring compliance across all operations, and reporting to the board on cyber security performance. Phillip acts as the primary point of contact for all cyber security matters, including liaison with the NCSC, certification bodies, and Client Organisations.

IT Support Provider

R&M's external IT support provider is responsible for the technical implementation and maintenance of cyber security controls, including firewall management, endpoint protection, patch deployment, backup management, and network monitoring. The IT provider operates under a service level agreement that specifies response times for security incidents and obligations for maintaining systems in line with Cyber Essentials requirements. Chris Walker is the designated IT contact responsible for the day-to-day management of R&M's IT infrastructure and for escalating security incidents to the Compliance Officer.

All Employees and Workers

Every person who accesses R&M's systems, devices, or data has a responsibility to follow the controls set out in this policy, to complete mandatory cyber security training, to report any suspected security incident immediately, and to exercise vigilance when handling data and using digital systems. Failure to comply with this policy may result in disciplinary action, up to and including termination of employment, and may also constitute a criminal offence under the Computer Misuse Act 1990 or a breach of the Data Protection Act 2018.

6. Technical Security Controls

Access Control and Authentication

Access to all R&M systems and data is governed by the principle of least privilege. Each user is assigned a unique account with permissions appropriate to their role. Administrator accounts are restricted to authorised IT personnel and are not used for day-to-day activities. Multi-factor authentication (MFA) is mandatory for all cloud services, remote access, email accounts, and any system that holds or processes sensitive data. Passwords must be a minimum of twelve characters, using a combination of upper and lower case letters, numbers, and special characters. Passwords must not be shared, reused across systems, or stored in unencrypted form. Access rights are reviewed quarterly and revoked immediately when an individual leaves the organisation or no longer requires access.

Device Security and Configuration

All company devices - including laptops, desktops, tablets, and mobile phones - are configured in accordance with NCSC secure configuration guidance. Default passwords and unnecessary user accounts are removed before deployment. Only authorised software may be installed on company devices. Automatic screen locking is enabled after five minutes of inactivity. All devices are encrypted using full-disk encryption. Personal devices may only be used to access company data with prior written approval and must meet the same security standards as company-issued equipment. USB drives and removable media require approval from the Compliance Officer before use.

Network Security

R&M's network infrastructure is protected by enterprise-grade firewalls and intrusion detection systems. Network traffic is monitored for anomalous activity. Guest and visitor Wi-Fi is segregated from the corporate network. Remote access to company systems is exclusively through encrypted VPN connections or approved secure remote desktop solutions. All wireless networks use WPA3 or WPA2-Enterprise encryption. Network configurations are reviewed at least annually and following any significant change to the IT environment.

Email and Phishing Protection

Email remains the primary vector for cyber attacks in the construction sector. R&M deploys email filtering and anti-phishing controls to detect and quarantine malicious emails before they reach users. All employees receive phishing awareness training as part of their induction and annual refresher programme. Simulated phishing exercises are conducted periodically to test awareness and identify individuals who may benefit from additional training. Employees must verify any request for financial transactions, changes to payment details, or transfer of sensitive information through a separate, trusted communication channel before acting on it.

Malware Protection

All endpoints - including servers, workstations, laptops, and mobile devices - are protected by centrally managed anti-malware software with real-time scanning and automatic definition updates. Application whitelisting is used where technically feasible to prevent execution of unauthorised software. Web filtering is applied to block access to known malicious websites and to restrict access to high-risk categories of web content.

Patch Management and Software Updates

All operating systems, applications, and firmware are maintained at supported versions. Critical and high-risk security patches are applied within fourteen days of release, in line with Cyber Essentials requirements. Where a patch cannot be applied within this timeframe due to compatibility or operational constraints, a documented risk assessment and compensating controls must be approved by the Compliance Officer. End-of-life software that no longer receives security updates is replaced on a planned basis. Automatic updates are enabled wherever technically feasible.

7. Data Protection and Information Security

Data Classification

All data handled by R&M is classified according to its sensitivity and the impact of its unauthorised disclosure, modification, or loss. Categories include: confidential (Client Organisation financial data, development appraisals, land valuations, personal data of residents and stakeholders), internal (project documentation, correspondence, commercial terms), and public (marketing materials, published planning documents). Controls for handling, storage, and transmission are applied proportionate to the classification of the data.

Public Sector and Client Organisation Data

R&M recognises that working within public sector frameworks involves handling data that belongs to or relates to Client Organisations, their residents, elected members, and communities. This includes sensitive land and property information, financial models, partnership financial data, personal data processed in connection with housing allocations or community engagement, and confidential commercial information shared through framework and client digital platforms. All such data is treated as confidential and is subject to the full range of controls set out in this policy. Where a Client Organisation specifies additional data security requirements through a call-off contract or data sharing agreement, R&M will comply with those requirements and, where necessary, implement supplementary controls.

Data Backup and Recovery

R&M maintains a comprehensive backup regime to protect against data loss from cyber attack, hardware failure, or human error. Critical business data is backed up daily to a secure, geographically separate cloud location. Backups are encrypted both in transit and at rest. Backup integrity is tested monthly through restoration exercises to verify that data can be recovered within acceptable timeframes. Backup retention periods are set in accordance with R&M's data retention schedule and any contractual or regulatory requirements. Backups are stored on systems that are isolated from the main network to protect against ransomware attacks that seek to encrypt or destroy backup data.

Secure Disposal

When equipment reaches end of life or is reassigned, all data is securely erased using NCSC-approved methods before the device is disposed of, recycled, or repurposed. Hard drives that cannot be reliably wiped are physically destroyed. Certificates of destruction are obtained and retained for audit purposes. Paper documents containing sensitive information are cross-cut shredded or disposed of through a certified confidential waste service.

8. Construction and Project-Specific Cyber Risks

The construction and property development sector faces a distinctive set of cyber risks that go beyond generic business IT threats. R&M has identified and addresses the following sector-specific risks:

- **Development appraisals and financial models** - these documents contain commercially sensitive valuations, profit projections, and land pricing that could cause significant financial harm if disclosed to competitors or the market. They are stored in encrypted, access-controlled environments and shared only through secure channels.
- **BIM and design data** - building information models and architectural designs represent significant intellectual property and contain detailed information about building layouts, security systems, and services. Access is restricted to project team members on a need-to-know basis.
- **Payment fraud and mandate fraud** - the construction sector is a prime target for invoice redirection fraud, where attackers impersonate subcontractors or suppliers and request changes to payment details. R&M requires verbal verification through a known contact number before processing any change to bank or payment details.
- Framework and client digital platforms - contract and cost management, social value tracking and reporting dashboards contain live project data. Access credentials for these platforms are managed under the same controls as all other system access, with MFA enabled and access revoked promptly when personnel change.
- **Site-based technology** - CCTV systems, site access controls, IoT sensors, and site Wi-Fi networks present potential attack surfaces. All site-based technology is configured in line with NCSC guidance, with default credentials changed, firmware updated, and network access segregated from corporate systems.
- **Supply chain compromise** - subcontractors and consultants who connect to R&M systems or handle project data may introduce cyber risk. Supply chain cyber security requirements are addressed in Section 9 of this policy.

9. Supply Chain Cyber Security

R&M's supply chain partners - including subcontractors, consultants, and professional advisors engaged on framework projects - handle project data, connect to shared platforms, and in some cases access R&M systems. A compromise of a supply chain partner's security can directly affect R&M and the Client Organisation. R&M manages supply chain cyber risk through the following measures:

- All supply chain partners who access R&M systems or handle sensitive project data are required to demonstrate that they have appropriate cyber security measures in place, proportionate to the nature and sensitivity of the data they handle

- For framework projects involving sensitive public sector data, R&M will give preference to supply chain partners who hold Cyber Essentials certification or can demonstrate equivalent controls
- Supply chain partners are required to report any cyber security incident that may affect R&M data or systems immediately upon discovery
- Data sharing with supply chain partners is governed by written agreements that specify security requirements, permitted uses, retention periods, and secure disposal obligations
- Access to shared project platforms is granted on a per-project, least-privilege basis and revoked at project completion or when a partner's engagement ends

Louis Howard, R&M's Procurement Manager at Enabl, incorporates cyber security requirements into the supply chain procurement and onboarding process, ensuring that partners are assessed for cyber risk before engagement and that contractual protections are in place.

10. Cyber Security Incident Response

Incident Reporting

All employees, subcontractors, and supply chain partners must report any suspected or confirmed cyber security incident immediately. Reportable incidents include but are not limited to: suspected phishing emails, malware infections, lost or stolen devices, unauthorised access to systems or data, data breaches, ransomware attacks, and any unusual system behaviour that may indicate a compromise. Reports should be made to:

- **Primary contact:** Chris Walker (IT Support) - for immediate technical response and containment
- **Escalation:** Phillip Hollingworth (H&S Adviser, Spectra Safety) - for governance, regulatory reporting, and coordination with senior management

Outside working hours, incidents should be reported by telephone to the numbers displayed on the R&M intranet and site welfare notice boards.

Incident Response Process

R&M maintains a documented Cyber Security Incident Response Plan that follows the NCSC's incident management guidance. The plan covers four phases:

- **Containment** - immediate actions to limit the spread and impact of the incident, which may include isolating affected systems, disabling compromised accounts, and blocking malicious network traffic
- **Assessment** - determining the nature, scope, and severity of the incident, identifying what data or systems have been affected, and assessing the potential impact on R&M, Client Organisations, and individuals
- **Remediation** - eradicating the threat, restoring affected systems from clean backups, resetting compromised credentials, and implementing additional controls to prevent recurrence
- **Recovery and lessons learned** - restoring normal operations, conducting a post-incident review to identify root causes and improvement actions, and updating policies, controls, and training as required

Regulatory Notification

Where a cyber security incident results in a personal data breach, R&M will assess whether notification to the Information Commissioner's Office (ICO) is required under the UK GDPR. Notifiable breaches - those likely to result in a risk to individuals' rights and freedoms - will be reported to the ICO within seventy-two hours of R&M becoming aware of the breach. Where a breach is likely to result in a high risk to affected individuals, those individuals will also be notified without undue delay. Where the incident affects Client Organisation data, the relevant Client Organisation will be informed immediately regardless of whether ICO notification is required, in accordance with R&M's partnership obligations and any applicable data processing agreement.

11. Business Continuity and Disaster Recovery

R&M maintains a business continuity plan that addresses the impact of a significant cyber security incident on the company's ability to operate and deliver its framework and project commitments. The plan includes:

- Identification of critical business systems and data, with recovery time objectives and recovery point objectives defined for each
- Documented procedures for restoring operations from backups in the event of ransomware, data destruction, or prolonged system outage
- Alternative working arrangements to enable project delivery to continue during an extended IT disruption, including offline access to critical project documentation and communication channels
- Regular testing of recovery procedures, with a full disaster recovery exercise conducted at least annually and results reported to the board
- Communication protocols for notifying Client Organisations, the Framework Manager, and supply chain partners of any disruption that may affect project delivery timelines

The business continuity plan is maintained by Phillip Hollingworth and reviewed annually alongside this policy. Lessons learned from incidents and exercises are used to update and improve the plan.

12. Training and Awareness

R&M's cyber security training programme ensures that all personnel understand the cyber threats relevant to their role and the controls they are expected to follow:

- **All employees** receive cyber security awareness training at induction, covering phishing recognition, password security, safe use of email and internet, data handling, reporting incidents, and the specific risks facing the construction sector. This training is refreshed annually through structured training sessions and toolbox talks on active sites.
- **Managers and directors** receive additional training on their responsibilities for enforcing cyber security controls within their teams, recognising social engineering attacks, and managing cyber incidents.
- **IT and administrative staff** with elevated system access receive role-specific training on secure system administration, access management, and the technical aspects of the Cyber Essentials controls.

- **Supply chain partners** are provided with a summary of R&M's cyber security requirements at project induction and are expected to ensure their own personnel are appropriately trained.

Training records are maintained by the Compliance Officer and reported to the board quarterly. Simulated phishing exercises are conducted at least twice annually to measure awareness levels and identify areas for improvement.

13. Acceptable Use of IT Systems

All users of R&M's IT systems must:

- Use company devices and systems primarily for business purposes; limited personal use is permitted provided it does not compromise security, productivity, or the company's reputation
- Not access, store, download, or transmit illegal, offensive, or unlicensed content using company systems or networks
- Lock screens and secure devices when leaving them unattended, even briefly
- Not connect unauthorised devices to the company network without approval from the IT support provider
- Not attempt to bypass, disable, or circumvent any security control, firewall, or access restriction
- Not install software, browser extensions, or applications without authorisation
- Report any request to share login credentials, bypass security controls, or take any action that conflicts with this policy

14. Remote and Mobile Working

R&M employees frequently work from construction sites, client offices, and home locations. Remote and mobile working introduces additional cyber risks that are managed through the following controls:

- All remote access to company systems must be through an approved VPN or secure remote desktop solution
- Company data must not be stored on personal devices unless those devices meet R&M's security standards and have been approved by the IT support provider
- Public Wi-Fi networks must not be used to access company systems or transmit sensitive data; mobile data or a personal hotspot should be used instead
- Physical security of devices must be maintained at all times - laptops must not be left visible in vehicles, and devices must be stored securely when not in use
- Any lost or stolen device must be reported immediately so that remote wipe can be initiated and access credentials can be revoked

15. Monitoring, Audit, and Continuous Improvement

R&M monitors its cyber security posture through the following mechanisms:

- Continuous automated monitoring of network activity, endpoint security status, and patch compliance through the IT support provider's management tools

- Quarterly review of access rights, user accounts, and administrative privileges to ensure they remain appropriate and that dormant accounts are disabled
- Annual Cyber Essentials recertification, providing an independent assessment of baseline controls
- Annual review of this policy by the Compliance Officer, with updates to reflect changes in the threat landscape, legislation, technology, or business operations
- Post-incident reviews following any cyber security event, with findings documented and improvement actions tracked to completion
- Board-level reporting on cyber security performance, including incident statistics, training completion rates, certification status, and improvement actions, at least quarterly

R&M is committed to continuous improvement in cyber security maturity and will benchmark its practices against NCSC guidance, industry standards, and the expectations of public sector Client Organisations. The progression from Cyber Essentials to Cyber Essentials Plus represents one step in this ongoing improvement journey, and further enhancements will be identified and implemented as the business and the threat landscape evolve.

16. Policy Review

This policy is reviewed annually by the Compliance Officer and approved by the Director. The next scheduled review date is June 2027. The policy will also be reviewed following any significant cyber security incident, any material change in legislation or regulatory guidance, any significant change in R&M's IT systems or business operations, or upon feedback from Client Organisations or the Framework Manager.

Approved and Signed

Name: Thom McKenna

Position: Director, R&M Property Group Ltd

Date: 24 June 2026

This policy will be published on the R&M Property Group Ltd website and available to all employees, supply chain partners, and framework clients upon request.