

R&M POLICY · DATA AND CYBER SECURITY

Supply Chain Cyber Security Assessment Procedure

R&M Property Group Ltd

Document	RM-DC-03
Reference	RM-SCCA-001
Version	1.0
Issued	June 2026
Next review	June 2027
Approved by	Thomas McKenna, Director
Website issue	22 October 2026

1. Purpose

This procedure sets out how R&M Property Group Ltd assesses, evaluates, and supports the cyber security arrangements of sub-contractors and suppliers within its supply chain. It ensures that any organisation given access to R&M's systems, data, or project information has proportionate cyber security controls in place, and that R&M provides appropriate guidance to its supply chain on cyber security expectations and best practice.

2. Scope

This procedure applies to all sub-contractors, suppliers, consultants, and third-party service providers who:

- Are given access to R&M's IT systems, cloud platforms, or project management software (including Autodesk Build, Microsoft 365, or any shared digital environment).
- Receive, store, or process personal data, confidential information, or commercially sensitive information on behalf of R&M.
- Connect their own devices or systems to R&M's network or site-based IT infrastructure.
- Handle building safety information that forms part of the golden thread under the Building Safety Act 2022.

The level of assessment applied is proportionate to the nature and extent of access granted - sub-contractors with no access to R&M systems or data are not required to complete the full assessment but are still expected to comply with the general cyber security requirements communicated at induction and pre-start meetings.

3. Responsibilities

3.1 Chris Walker, IT Support

- Manages the technical aspects of granting and revoking supply chain access to R&M systems.
- Reviews the technical responses to cyber security pre-qualification questions.
- Advises the Procurement Manager on the adequacy of a sub-contractor's cyber security arrangements.
- Provides technical guidance to supply chain partners on R&M's IT security requirements.

3.2 Louis Howard, Procurement Manager (Enabl)

- Issues the cyber security pre-qualification questions as part of the sub-contractor selection process.
- Records and retains the assessment outcomes in the approved supplier register.
- Ensures that sub-contract orders and agreements include the cyber security requirements set out in this procedure.
- Escalates concerns about a sub-contractor's cyber security arrangements to the Director.

3.3 Thomas McKenna, Director

- Approves this procedure and any updates.

- Makes final decisions on the engagement of sub-contractors where cyber security concerns have been identified.

4. Pre-Qualification Cyber Security Questions

The following questions are included in R&M's pre-qualification questionnaire for sub-contractors and suppliers who will have access to company systems, data, or project information. Responses are assessed by Chris Walker (IT Support) and Louis Howard (Procurement Manager).

Question 1 - Cyber Security Policy

Does your company have a cyber security policy or information security policy that is approved by a director or senior manager and reviewed at least annually?

- **Expected evidence:** a copy of the policy, or confirmation that one exists with the date of last review.

Question 2 - Cyber Essentials Certification

Does your company hold a current Cyber Essentials or Cyber Essentials Plus certificate, or an equivalent information security certification (e.g. ISO 27001)?

- **Expected evidence:** certificate number and expiry date, or a copy of the certificate.

Question 3 - Access Controls and Passwords

Does your company enforce strong password requirements and use multi-factor authentication (MFA) on business email, cloud platforms, and remote access connections?

- **Expected evidence:** confirmation of password policy and MFA usage.

Question 4 - Software Updates and Malware Protection

Does your company keep all software, operating systems, and antivirus/anti-malware protection up to date, with patches applied promptly?

- **Expected evidence:** confirmation of patching policy or automatic update arrangements.

Question 5 - Data Backup

Does your company back up critical business data regularly, and are backups stored separately from the live system (off-site or in a separate cloud region)?

- **Expected evidence:** confirmation of backup frequency, storage location, and testing regime.

Question 6 - Incident Response

Does your company have a process for responding to cyber security incidents, including how you would notify R&M if an incident affected data or systems shared with us?

- **Expected evidence:** summary of incident response process and notification commitment.

Question 7 - Employee Awareness

Do your employees receive cyber security awareness training, including guidance on identifying phishing emails and social engineering attempts?

- **Expected evidence:** confirmation of training arrangements and frequency.

Question 8 - Remote and Home Working

If your employees work remotely or from home, do you have controls in place to secure remote access to your company systems (e.g. VPN, encrypted connections, guidance on securing home networks)?

- **Expected evidence:** confirmation of remote working controls.

Question 9 - Data Protection

Does your company have a data protection policy and is your company registered with the Information Commissioner's Office (ICO)?

- **Expected evidence:** ICO registration number, or confirmation of registration status.

Question 10 - Previous Incidents

Has your company experienced a cyber security incident or data breach in the last 24 months that affected client data, project information, or business-critical systems? If yes, please provide a brief summary of the incident and the remedial actions taken.

- **Expected evidence:** yes/no declaration. If yes, a brief summary.

5. Evaluation and Scoring Methodology

Responses to the pre-qualification questions are evaluated using a proportionate, risk-based approach. The assessment is not intended to impose enterprise-level security requirements on small trade sub-contractors, but to confirm that basic, proportionate controls are in place.

5.1 Scoring

Each question is scored as follows:

- **Meets requirement (Green) -** the sub-contractor has the control in place and can provide evidence or a clear confirmation.
- **Partially meets requirement (Amber) -** the sub-contractor has some controls in place but there are gaps, or the control is informal rather than documented. The sub-contractor is asked to address the gap within an agreed timeframe.
- **Does not meet requirement (Red) -** the sub-contractor does not have the control in place and cannot demonstrate an alternative arrangement. This is escalated to the Director for a decision on whether to proceed, with conditions if appropriate.

5.2 Minimum Requirements

For sub-contractors who will have access to R&M's systems or handle personal or confidential data, the following are minimum requirements:

- A cyber security or information security policy in place (Question 1) - or a written commitment to adopt one within 3 months of engagement.
- Antivirus and software updates applied (Question 4).
- A process for notifying R&M of incidents affecting shared data or systems (Question 6).
- ICO registration if processing personal data (Question 9).

Holding Cyber Essentials certification (Question 2) is valued but not mandatory for all sub-contractors. Where a sub-contractor does not hold certification, R&M assesses their individual

responses to determine whether their controls are adequate for the level of access being granted.

5.3 Proportionality

The depth of assessment is proportionate to the risk:

- **High access -** sub-contractors with direct access to R&M cloud platforms (Autodesk Build, Microsoft 365), personal data, or building safety information: full 10-question assessment required.
- **Moderate access -** sub-contractors who receive project documents or drawings electronically but do not have login access to R&M systems: questions 1, 4, 5, 6, and 9 required.
- **Low or no access -** trade sub-contractors with no access to R&M systems or data: general cyber security requirements communicated at pre-start meeting and site induction. No formal questionnaire required.

5.4 Record Keeping

Assessment outcomes are recorded in R&M's approved supplier register alongside other pre-qualification information. Assessments are reviewed at least every 12 months for sub-contractors on ongoing engagements, or when a sub-contractor's scope of access changes. Records are retained for the duration of the engagement plus 6 years.

6. Ongoing Monitoring

Cyber security is not assessed only at pre-qualification. R&M monitors supply chain cyber security on an ongoing basis through the following mechanisms:

- Annual reassessment - sub-contractors with system access are asked to confirm that their arrangements remain in place and to report any material changes.
- Incident notification - sub-contracts include a requirement to notify R&M immediately of any cyber security incident that could affect R&M's data, systems, or project information.
- Access reviews - Chris Walker reviews the list of supply chain users with access to R&M systems quarterly and revokes access for any organisation no longer engaged or where access is no longer required.
- Performance monitoring - any cyber security incident, near-miss, or concern raised during an engagement is recorded and considered at the next pre-qualification review.

7. Information and Guidance Provided to the Supply Chain

R&M provides the following information and guidance to its supply chain to support good cyber security practice:

7.1 At Pre-Qualification

- A copy of this procedure, setting out R&M's expectations and the assessment process.
- A summary of R&M's Cyber Security Policy (RM-CSP-001), highlighting the key requirements that apply to supply chain partners.
- Where a sub-contractor scores Amber on any question, specific written guidance on what improvement is expected and the timeframe for achieving it.

7.2 At Pre-Start and Site Induction

All sub-contractors, including those not subject to the full questionnaire, receive the following cyber security guidance as part of the pre-start meeting and site induction:

- Do not connect personal or unauthorised devices to R&M's site network or Wi-Fi without approval.
- Do not share login credentials for any R&M system - each user must have their own account.
- Report any suspected cyber security incident (phishing email, suspicious activity, lost device) to the site manager or Chris Walker immediately.
- Do not download, copy, or share project information, drawings, or building safety data outside the approved platforms (Autodesk Build) without written permission.
- Photographs taken on site must not include confidential or security-sensitive information and must not be shared on social media without approval.
- USB drives and portable storage devices must not be used on R&M systems without prior approval.

7.3 Ongoing Support

- Where R&M identifies a significant cyber security threat relevant to the construction sector (for example a widespread phishing campaign or a vulnerability in commonly used software), a brief alert is circulated to active supply chain partners.
- Sub-contractors are encouraged to work towards Cyber Essentials certification. R&M can provide guidance on the certification process on request.
- Where a sub-contractor experiences a cyber security incident and notifies R&M, Chris Walker provides practical support and guidance to help contain and resolve the incident where it may affect R&M's data or project information.

8. Contractual Requirements

Sub-contract orders and agreements include the following cyber security provisions:

- A requirement to maintain proportionate cyber security controls for the duration of the engagement.
- A requirement to notify R&M immediately of any cyber security incident that could affect R&M's data, systems, or project information.
- A requirement to comply with R&M's Cyber Security Policy and this procedure when accessing R&M's systems or handling R&M's data.
- A right for R&M to revoke system access immediately if a sub-contractor's cyber security arrangements are found to be inadequate or if a breach occurs.
- A requirement to return or securely delete all R&M data on completion of the engagement.

9. Escalation

Where a sub-contractor's cyber security arrangements are assessed as inadequate (Red on any minimum requirement), or where a sub-contractor refuses to engage with the assessment process, the matter is escalated to Thomas McKenna (Director) for a decision. The Director may:

- Approve engagement with conditions - for example, restricting the sub-contractor's access to specific systems, requiring improvement within a defined timeframe, or requiring the sub-contractor to use R&M-provided devices.
- Decline engagement - where the risk to R&M's data, systems, or clients is too high and cannot be adequately mitigated.
- Suspend access - for an existing sub-contractor where a material deterioration in their cyber security arrangements is identified or an incident occurs.

Escalation decisions and their rationale are recorded in the approved supplier register.

10. Review

This procedure is reviewed annually by Chris Walker, Louis Howard, and Thomas McKenna, or sooner if there is a significant change in the cyber threat landscape, a supply chain cyber security incident, or a material change to R&M's IT systems or regulatory obligations. All changes are approved by the Director.

11. Related Documents

- Cyber Security Policy (RM-CSP-001)
- Data Protection Policy and Privacy Notice (RM-DPP-001)
- Sub-Contractor Selection and Monitoring Policy
- Quality Management Policy (RM-QMP-001)
- Risk Management Policy

Signed and Approved:

Thomas McKenna

Director, R&M Property Group Ltd

Date: June 2026