

CYBERSECURITY POLICY

Company Name: Evolve Document Solutions Limited

Last Reviewed: 13th October 2025

Next Review Due: 12th October 2026

Policy Owner: Daniel Maddox - Director

1. PURPOSE

Evolve Document Solutions Limited recognises that information and IT systems are critical to our business and to the trust our clients place in us. This policy sets out how we protect our systems, networks, and data from cyber threats. Our goal is to ensure confidentiality, integrity, and availability of data in line with the UK GDPR, the Data Protection Act 2018, and the principles of the UK Government's Cyber Essentials scheme¹.*

2. SCOPE

This policy applies to:

- All employees, contractors, and agency staff.
- All company IT systems, devices, software, and networks.
- All client and company data processed, stored, or transmitted by us.
- All third-party IT service providers who manage or host data on our behalf.

3. OUR COMMITMENTS

Evolve Document Solutions will:

- Protect company and client data against unauthorised access, disclosure, alteration, or destruction.
- Apply appropriate security controls across our IT systems.
- Comply with relevant legislation and client requirements.

- Train staff to understand cybersecurity risks and their responsibilities.
- Maintain business continuity through effective data backup and recovery processes.

4. ACCESS & AUTHENTICATION

- Access to systems and data will be granted on the principle of least privilege^{2*}.
- Strong, unique passwords must be used for all accounts and changed regularly.
- Multi-factor authentication (MFA) will be implemented wherever possible.
- Accounts of leavers will be deactivated promptly.

5. DATA PROTECTION & BACKUP

- All client and company data must be stored securely, with encryption applied both at rest and in transit.
- Backups will be performed daily and tested at least quarterly to ensure data can be restored.
- Portable storage devices (e.g., USB drives) must not be used unless encrypted and approved.
- Data will be retained and deleted in line with GDPR and company retention schedules.

6. USE OF IT SYSTEMS

- Company IT equipment and systems are to be used responsibly and primarily for business purposes.
- Emails must be handled carefully to avoid phishing or malware attacks.
- Employees must not install unauthorised software.
- Remote working must only be carried out using secure connections (e.g., VPN, company-approved devices).
- All devices must be protected by antivirus and regular security updates.

7. INCIDENT RESPONSE

- Any suspected cybersecurity incident, data breach, or phishing attempt must be reported immediately to the Managing Director or appointed IT contact.
- All incidents will be logged and investigated.
- Where personal data is affected, GDPR breach notification requirements will be followed.
- Lessons learned from incidents will be used to strengthen security controls.

8. THIRD PARTIES & SUPPLY CHAIN

- Third-party IT providers must demonstrate that they meet appropriate security standards (e.g., Cyber Essentials or equivalent).
- Contracts with suppliers handling client or company data must include appropriate data protection and security requirements.
- Due diligence checks will be carried out on new IT suppliers before engagement.

9. TRAINING & AWARENESS

- All staff will receive cybersecurity awareness training, including how to identify phishing emails, use strong passwords, and report incidents.
- Training will be refreshed annually and after significant changes to systems or policies.
- Staff responsibilities for safeguarding data will be reinforced regularly.

10. REVIEW

This policy will be reviewed annually, or sooner if required by legislation, client requirements, or business changes.

APPROVAL

Signed: *Don Madge* (Managing Director)

Date: *1/11/2025*