



CYBER SECURITY POLICY

Connect Skilled Contractor Service Ltd

1. Purpose

This policy defines the cyber security framework used by Connect Skilled Contractor Service Ltd to protect its information systems, digital assets, client data, and operational continuity against cyber threats, unauthorised access, data loss, and misuse.

The company recognises cyber security as a core business risk and implements controls aligned with UK GDPR, the Data Protection Act 2018, and recognised industry best practice.

2. Scope

This policy applies to:

- All employees, directors, contractors, subcontractors, and third-party service providers
- All IT systems, devices, software, cloud platforms, and communication tools used for business purposes

- All data held, processed, or transmitted by the organisation
-

3. Cyber Security Governance

1. The Managing Director holds overall responsibility for cyber security compliance.
 2. Operational responsibility is delegated to a nominated IT/security lead.
 3. Cyber security risks are reviewed at least quarterly.
 4. Security controls are proportionate to the size and risk profile of the business.
 5. Any significant security incident must be escalated immediately to senior management.
-

4. Access Control

6. Access to systems is restricted on a strict “least privilege” basis.
 7. User accounts are unique and must not be shared.
 8. Access rights are reviewed when staff change roles or leave the company.
 9. Immediate revocation of access occurs upon termination of employment or contract.
 10. Administrative access is limited to authorised personnel only.
-

5. Password and Authentication Controls

11. Strong passwords are required for all systems (minimum complexity enforced).
12. Passwords must not be reused across systems.

13. Multi-factor authentication (MFA) is enabled wherever technically possible.
 14. Passwords must be stored securely using approved password management tools.
-

6. Device and Endpoint Security

15. All business devices must have up-to-date antivirus/anti-malware protection.
 16. Operating systems and applications must be regularly patched and updated.
 17. Devices must be protected with screen locks and automatic timeout settings.
 18. Lost or stolen devices must be reported immediately.
-

7. Network Security

19. Firewalls are used to protect internal systems and network traffic.
 20. Wi-Fi networks are secured with strong encryption and passwords.
 21. Remote access is only permitted via secure, authenticated connections.
 22. Public or unsecured Wi-Fi must not be used for business operations without a secure VPN.
-

8. Email and Communication Security

23. Email systems are protected against phishing, spoofing, and malware.
24. Employees must verify suspicious emails before clicking links or attachments.

25. Sensitive data must not be sent via unsecured email without encryption or approval.
-

9. Data Backup and Recovery

26. Business-critical data is backed up regularly.
 27. Backups are stored securely and protected from unauthorised access.
 28. Recovery procedures are tested periodically to ensure business continuity.
-

10. Incident Management

29. All cyber security incidents must be reported immediately to management.
 30. Incidents include suspected phishing, data loss, unauthorised access, or malware infection.
 31. All incidents are logged, investigated, and documented.
 32. Where required, ICO reporting procedures are followed within statutory timeframes.
-

11. Third-Party Security

33. Suppliers and subcontractors are assessed for cyber security risk before engagement.
 34. Data processing agreements are used where third parties handle personal data.
 35. Third parties must demonstrate appropriate technical and organisational controls.
-

12. Training and Awareness

- 36. Staff receive basic cyber security awareness training upon onboarding.
 - 37. Refresher training is provided annually or when risks change.
 - 38. Employees are educated on phishing, social engineering, and secure data handling.
-

13. Monitoring and Review

- 39. Security controls are monitored for effectiveness.
 - 40. This policy is reviewed at least annually or after any major security incident.
-

14. Compliance

- 41. Failure to comply with this policy may result in disciplinary action.
 - 42. The company complies with UK GDPR, Data Protection Act 2018, and relevant cyber security standards.
-

15. Approval

Approved by: Managing Director

Company: Connect Skilled Contractor Service Ltd

Review frequency: Annually