Cyber Security Policy Template

For recruitment businesses | Prepared by TWC IT Solutions for The Recruitment Network members

Organisation: [Company name] Policy owner: [Name/role] Approved: [Date] Review due: [Date]

This adaptable policy reflects the layered security principles used in TWC's managed cyber security approach. It is not a copy of TWC's internal ISO 27001 policies. The adopting organisation must confirm that each control is implemented, assign responsibilities and approve the final wording.

1. Purpose and responsibilities

[Company name] will protect its systems and the personal and commercially sensitive information entrusted to it, including candidate CVs, identification documents, payroll details, client records and recruitment platform data. Management is accountable for security; [Security lead/IT provider] maintains controls; all staff and contractors must comply with this policy and report concerns promptly.

2. Accounts and access

Use individual accounts, strong unique passwords and multi-factor authentication for Microsoft 365, recruitment systems and other important services. Do not share accounts or authentication codes. Access must be limited to job requirements, reviewed periodically and removed promptly when someone leaves or changes role. Privileged access must be restricted and separately controlled.

3. Devices and remote working

Only approved, appropriately secured devices may access company information. Devices must use supported software, screen locks, encryption where supported and centrally managed endpoint protection. Apply security updates promptly; address high-risk or critical vulnerabilities within 14 days of a fix becoming available, where required by the applicable Cyber Essentials standard. Enable host and network firewalls, remove unnecessary software and services, change default credentials and restrict administrative access. Lost devices must be reported immediately.

4. Email, phishing and safe working

Treat unexpected links, attachments, payment requests and changes to bank details with caution. Independently verify unusual requests using a trusted contact method. Do not disable security software or bypass warnings. Staff must complete assigned security awareness training and report suspicious messages without delay.

5. Candidate, client and recruitment data

Collect and use only the information needed for legitimate recruitment activities. Store CVs, candidate records, identity documents and client information in approved systems, with appropriate access permissions and retention periods. Share sensitive data only through authorised channels. Follow applicable UK GDPR and data protection procedures, including secure deletion and reporting suspected breaches.

6. Recruitment platforms and suppliers

Access to applicant tracking systems (ATS), job boards, payroll tools and other third-party services must be authorised and reviewed. Before adopting a supplier, assess its security, data-handling practices and access requirements. Integrations and exports must be approved, and unnecessary data transfers avoided.

7. AI and automation

Use only AI services approved by [Company name]. Do not upload candidate personal data, confidential client information, credentials or commercially sensitive material into public AI tools without explicit authorisation and appropriate safeguards. Review AI-generated outputs for accuracy, bias and confidentiality before use, particularly in candidate assessment or client communications.

8. Protection, monitoring and recovery

Maintain proportionate, layered protection, including firewalls, secure configuration, endpoint and email security, vulnerability monitoring, security updates, appropriate alerting, tested backups and recovery arrangements. The organisation and its IT provider must agree who monitors alerts, maintains controls and coordinates recovery.

9. Incident reporting and response

Immediately report suspected phishing, account compromise, lost devices, ransomware, unauthorised access or accidental disclosure to [Security contact and telephone/email]. Preserve evidence and follow the incident response process. The designated privacy lead must assess personal data breaches promptly and, where legally required, notify the ICO without undue delay and within 72 hours of becoming aware; affected individuals must also be informed where the legal threshold is met.

10. Compliance and review

Breaches may result in disciplinary or contractual action. Exceptions require written approval by [Policy owner]. Review this policy at least annually and after a material incident or business change. Reference frameworks: NCSC Cyber Essentials (firewalls, secure configuration, security updates, access control and malware protection), NCSC small-business guidance and ICO personal data breach guidance. This template alone does not demonstrate certification or legal compliance.

Approval and local implementation

Approved by: _____ Date: _____ Security contact: _____

Before issuing: confirm these controls operate in practice; identify approved systems and AI tools; set reporting contacts, retention rules and training requirements; and obtain management approval. Adapt any security-update deadlines to the current Cyber Essentials requirements.

TWC IT Solutions | Complimentary TRN member resource. For an independent cyber security, Microsoft 365 and AI readiness review, contact richard@twcitsolutions.com.