Cyber Security & Responsible AI

Practical guidance for The Recruitment Network members

Protecting recruitment businesses

Recruitment organisations rely on the confidentiality, availability and integrity of candidate records, client information, payroll details, commercial correspondence and recruitment platforms. Cyber security should therefore be approached as an ongoing business responsibility, not simply the purchase of antivirus software or the completion of an annual compliance exercise. The right approach is proportionate to the size, activities and risk profile of each business.

Where to begin

Cyber Essentials provides a useful, recognised baseline for UK organisations. It focuses attention on fundamental technical controls, including secure configuration, access control, security updates, malware protection and firewalls. Cyber Essentials Plus adds independent technical verification. Neither certification should be mistaken for a complete security or resilience programme.

Begin with an independent assessment of your existing systems, Microsoft 365 configuration, recruitment software, devices, suppliers and working practices. Establish who owns each risk, which controls already exist and where the most significant gaps lie. Prioritise improvements according to business impact rather than adding technology without a clear purpose.

The key areas to address

Identity and access: Require multi-factor authentication, review administrator privileges and use Conditional Access where appropriate. Remove access promptly when staff leave, and review external and third-party access.

Devices and remote working: Maintain supported, updated and protected laptops and mobiles. Use device management and appropriate controls for personal devices accessing business data.

Email and phishing: Strengthen email filtering and authentication, protect against impersonation and payment diversion, and give staff a clear route to report suspicious messages.

Human risk: Use regular, relevant education and phishing simulations, supported by constructive feedback and measurable improvement rather than one-off annual training.

Monitoring and response: Ensure alerts are reviewed, incidents have named owners, and there is a practical plan for containment, communication and recovery.

Backup and continuity: Back up critical business data, understand what is and is not protected in Microsoft 365 and recruitment platforms, and test restoration. Plan how the business will operate during an email, ATS or connectivity outage.

Suppliers and data: Review ATS, CRM, payroll and other suppliers; restrict unnecessary data sharing, define retention periods and ensure appropriate data protection arrangements.

Artificial intelligence: opportunity and risk

AI can help recruitment businesses draft job adverts, summarise information, support research and improve administrative efficiency. However, public AI tools and connected assistants can also introduce risks involving candidate confidentiality, personal data, inaccurate outputs, bias, intellectual property and unauthorised disclosure of client information. AI-generated phishing, convincing impersonation and deepfake voice or video are also changing the threat landscape.

Every recruitment business should adopt a straightforward acceptable-use policy covering approved AI services, permitted information, human review and accountability. Staff should not enter candidate CVs, identity documents, salary details, client-confidential information or other personal data into unapproved AI tools. Before deploying AI in candidate screening or decision-making, assess fairness, transparency, data protection obligations, supplier terms and the need for meaningful human oversight.

Where AI tools connect to Microsoft 365 or other internal systems, review permissions and existing information-sharing arrangements first. An AI assistant may make poorly controlled data easier to discover, so access governance and data classification remain essential.

A practical next step

For most members, the sensible first step is a short, independent security and AI-readiness review. This should produce a prioritised action plan covering immediate risks, Cyber Essentials readiness, Microsoft 365 and device controls, staff behaviour, business continuity and responsible AI use. Improvements can then be introduced in manageable stages with clear ownership, realistic costs and regular review.

TWC IT Solutions supports TRN members with consultancy-led technology, cyber security, human risk management and resilience services. The aim is to help each business establish controls that are appropriate, effective and sustainable, without unnecessary complexity.