Foundations Search

Cybersecurity Compliance Policy

v2.0 • March 2026

Cyber talent for critical infrastructure.
Decreasing time & effort. Increasing quality. Without compromise.

1. Introduction and Purpose

This Cybersecurity Compliance Policy outlines the guiding principles, practices, and standards that Foundations Search adheres to in order to protect and maintain the confidentiality, integrity, and availability of our information systems, client data, and candidate information.

As a specialist cyber security recruitment firm operating across critical national infrastructure sectors, Foundations Search recognises the heightened importance of robust cybersecurity practices. We are committed to maintaining the trust of our clients, candidates, and stakeholders across the UK and international markets.

1.1 Document Control

Item	Detail
Policy Owner	Laurence Connor, Operations Director
Approval Date	1 March 2026
Review Frequency	Annual
Next Review Date	1 March 2027
Classification	Internal — All Staff

2. Scope

This Policy applies to all employees, contractors, consultants, and partners of Foundations Search who have access to company information systems, data, and network infrastructure. It also extends to third-party service providers who process data on our behalf.

3. Roles and Responsibilities

- **Senior Management:** ensure allocation of resources and support for cybersecurity initiatives, set the security-first culture, and approve policy updates.
- **Operations Director:** acts as the designated security lead, oversees policy implementation, and manages incident response.
- **All Employees:** adhere to this Policy, participate in mandatory cybersecurity training, and report any suspected incidents immediately.
- **Third-party Providers:** comply with our security requirements as outlined in their data processing agreements.

4. Data Classification and Handling

All information processed by Foundations Search is classified into one of the following categories:

- **Confidential:** client details, candidate profiles (including CVs, clearance information, and assessment results), contracts, financial information, and proprietary company data. Access restricted to authorised personnel only.
- **Internal Use:** non-sensitive operational information, internal communications, and process documentation. Available to all staff but not for external distribution.
- **Public:** marketing materials, published insights, job advertisements, and website content.

All employees must ensure that data is stored, transmitted, and disposed of in a manner appropriate to its classification. Particular care must be taken with candidate data that includes security clearance levels, vetting status, or other sensitive personal information.

5. Access Control

- **Authentication:** all users must use strong, unique passwords combined with multi-factor authentication (MFA) on all business-critical systems.
- **Principle of least privilege:** access to confidential data is restricted to authorised personnel on a need-to-know basis.
- **Access reviews:** user access rights are reviewed quarterly and upon any change of role or departure.
- **Password policy:** passwords must be a minimum of 14 characters, changed every 180 days, and never reused across systems.

6. Security Awareness and Training

All Foundations Search employees undergo cybersecurity awareness training on joining the company and annually thereafter. Training covers:

- Phishing and social engineering recognition.
- Secure handling of candidate and client data.
- Password hygiene and multi-factor authentication.
- Incident reporting procedures.
- Sector-specific security considerations for CNI recruitment.

Additional targeted briefings are provided when emerging threats are identified that may impact our operations or the sectors we serve.

7. Incident Response

Foundations Search maintains a documented incident response plan covering:

- **Identification:** monitoring and detection of potential security incidents.
- **Containment:** immediate steps to limit the scope and impact of an incident.
- **Eradication:** removal of the threat from our systems.
- **Recovery:** restoration of systems and data to normal operations.
- **Notification:** informing affected parties, the ICO (within 72 hours where required), and relevant authorities.
- **Post-incident review:** analysis of root cause and implementation of preventive measures.

All suspected security incidents must be reported immediately to the Operations Director. Even minor concerns should be raised — early reporting enables faster containment.

8. Audits and Assessments

To ensure ongoing compliance and security, Foundations Search undertakes:

- Annual cybersecurity audits of our systems and processes.
- Quarterly vulnerability assessments of external-facing systems.
- Ongoing monitoring of access logs and system alerts.
- Findings are reviewed and remediation actions are tracked to completion.

9. Data Protection and Privacy

Foundations Search is compliant with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and applicable data protection laws in all jurisdictions where we operate. We commit to:

- Collecting only data that is necessary for our legitimate recruitment operations.
- Protecting the rights of data subjects, including candidates, clients, and employees.
- Ensuring that any cross-border data transfer is secure and compliant with appropriate safeguards.
- Maintaining a Record of Processing Activities (ROPA) as required by Article 30 of UK GDPR.

Our full privacy practices are detailed in our separate Privacy Policy & GDPR document.

10. Third-party and Vendor Management

Foundations Search evaluates the cybersecurity posture of all third-party vendors before engagement. Vendors who process personal data on our behalf must:

- Demonstrate compliance with relevant security standards.
- Enter into a Data Processing Agreement (DPA) that meets UK GDPR requirements.
- Undergo periodic security reviews during the relationship.

11. Physical Security

Secure access controls are implemented at all Foundations Search premises. All company-owned devices must be stored securely when not in use, encrypted at rest, and protected by screen locks. Remote working arrangements must comply with our remote access security guidelines.

12. Backup and Disaster Recovery

Regular automated backups of critical data are performed, with periodic restoration tests to verify integrity. Critical data is stored across geographically separated, encrypted cloud infrastructure. Our business continuity plan ensures operations can resume within defined recovery time objectives.

13. Policy Review

This Policy is reviewed annually or following significant changes to our operations, the threat landscape, or the regulatory environment. All staff are notified of material changes.

14. Violations

Any violations of this Policy may result in disciplinary action, up to and including termination of employment. Serious breaches may be reported to relevant authorities and law enforcement.

Protecting our clients, candidates, and company data is of paramount importance to Foundations Search. We are dedicated to ensuring the security, confidentiality, and integrity of our information systems.

Signed,

Laurence Connor

Operations Director, Foundations Search

1 March 2026