athona

Information Security Policy for Athona

Introduction

This Information Security Policy (the "Policy") establishes the framework for managing information security risks within Athona (the "Company"), Athona is a Recruitment Agency providing qualified Healthcare and Education staff to the public and private sector. Athona Ltd provides temporary, contract and permanent staff and insourcing contracts to the Medical, Healthcare and Nursing markets in the UK and Internationally. Athona Education Ltd supplies Education Professionals on a temporary, contract and permanent basis to UK schools and Nurseries.

Purpose

The Policy protects the confidentiality, integrity, and availability of information assets, including personal data of candidates, clients, and employees, against unauthorised access, disclosure, alteration, destruction, or loss. It promotes a culture of security awareness, supports business continuity, and ensures compliant recruitment practices, such as secure data sharing with clients and third-party platforms.

The primary objectives are to:

- Safeguard sensitive information in high-risk recruitment activities (e.g. handling CVs, pre-screening compliance information, salary details, and client contracts).
- Mitigate threats like phishing, insider risks, and data breaches.
- Foster ethical and secure operations.

Regulatory and Standards Compliance

This Policy aligns with key UK regulations and international standards:

- **UK General Data Protection Regulation (UK GDPR)** and **Data Protection Act 2018 (DPA 2018)**: Mandating lawful, secure processing of personal data with accountability for controllers / processors, including technical / organisational measures (Articles 5, 24, 25, 32).
- **Privacy and Electronic Communications Regulations (PECR) 2003**: Governing secure electronic communications and opt-in consent for marketing.
- **Employment Agencies and Employment Businesses Regulations 2010**: Ensuring ethical handling of candidate data.
- **ISO/IEC 27001:2022**: Providing a systematic Information Security Management System (ISMS) for risk management, continual improvement, and certification.

The Company commits to fulfilling these obligations through documented measures, risk assessments, and audits. Non-compliance may result in fines, disciplinary action, legal penalties, or reputational harm.

Scope

This Policy applies to:

- All employees, contractors, temporary staff, and third-party vendors (e.g. job boards, ATS providers like Salesforce and RDB) who access, process, or handle Company information.
- All information assets, including physical, digital, and paper-based records (e.g. candidate databases, client contracts).
- All Company locations, remote work environments, and cloud-based systems used in recruitment.

Exclusions: Client-owned systems unless specified in contracts or Data Processing Agreements (DPAs).

Definitions

- **Confidentiality**: Ensuring information is accessible only to authorised individuals.
- **Integrity**: Protecting information from unauthorised modification or destruction.
- **Availability**: Ensuring timely, reliable access to information for authorised users.
- **Personal Data**: Any information relating to an identified or identifiable natural person (e.g. candidate contact details, health information under UK GDPR Article 9).
- **Information Asset**: Any data, document, or system of business value (e.g. CRM databases).
- **Data Breach / Incident**: Any event compromising security (e.g. unauthorised access, phishing attack).
- **Special Category Data**: Sensitive personal data requiring enhanced protection (e.g. diversity or health details).

Policy Statements

Information Classification and Handling

- Classify information by sensitivity: External use (e.g. job adverts), Internal use (e.g. operational guidelines), Confidential (e.g. client pricing), Restricted (e.g. special category personal data).
- Handling rules:
    - Encrypt Restricted/Confidential data at rest (e.g., AES-256) and in transit (e.g., TLS 1.3/HTTPS).
    - Use pseudonymisation/anonymisation where feasible (e.g. during CV screening).
    - Secure disposal: Shred paper records; securely wipe digital files per retention schedules compliant with DPA 2018.
    - Data sharing with clients / third parties requires DPAs (UK GDPR Article 28) and candidate / client consent.

Access Control

- Follow the principle of least privilege: Role-based access only (e.g. recruiters view candidate documents, compliance manage candidate documents).
- Mandate multi-factor authentication (MFA) for all systems, including email and remote VPN access.
- Review user accounts quarterly (or immediately on role / termination changes); revoke access within 24 hours of departure.
- Verify identities for data subject requests (e.g. access under UK GDPR Article 15) and remote logins.

Risk Management

- Conduct annual risk assessments and Data Protection Impact Assessments (DPIAs) for high-risk activities (e.g. AI candidate matching, bulk data exports), per ISO 27001 Annex A.8 and UK GDPR Article 35.
- Prioritise recruitment-specific threats (e.g. phishing, insider leaks) with proportionate controls, balancing costs and harm.
- Develop Business Continuity Plans (BCP) and Disaster Recovery (DR) with <4-hour Recovery Time Objective (RTO) for critical systems (e.g. applicant databases) and

Physical and Environmental Security

- Implement access controls (e.g., keycards, CCTV, visitor logging) for offices and locked storage for paper records.
- Secure portable devices (e.g., laptops, mobiles): Full-disk encryption, remote wipe, and endpoint protection (antivirus, firewall).
- Environmental safeguards (e.g., fire suppression, UPS) for on-site/cloud infrastructure.

Human Resources Security

- Perform background checks and require NDAs for new hires covering data protection and confidentiality.
- Mandatory annual security awareness training on UK GDPR, phishing, and recruitment-specific risks (e.g., secure CV sharing); track 100% completion.
- Exit procedures: Immediate access deactivation, device return, and knowledge transfer within 24 hours.

Communications and Operations Security

- Use secure channels for transfers (e.g., no unencrypted attachments; prefer portals for client data sharing).
- Monthly vulnerability scans, timely patching, and system updates per ISO 27001 Annex A.12.6.

- Log/monitor access events for 6-12 months with anomaly alerts (e.g., unusual data exports); retain for audits.

Data Protection and Privacy

- Process data per UK GDPR principles (lawful basis, minimisation, purpose limitation); provide clear privacy notices.
- Fulfil data subject rights (e.g., erasure under Article 17) within one month.
- Obtain explicit opt-in for marketing (PECR); apply Privacy by Design to new tools (e.g., DPIAs for AI screening).
- Limit data collection to essentials (e.g., application forms).

Incident Management

- Report suspected incidents (e.g., lost device with candidate data) immediately to the Information Security Officer (ISO) or Data Protection Officer (DPO).
- Response process (ISO 27001 Annex A.16): Assess, contain, eradicate, recover; notify ICO within 72 hours for high-risk breaches (UK GDPR Articles 33-34) and affected individuals without delay.
- Conduct post-incident reviews for lessons learned.

Supplier Relationships

- Assess third-party risks (e.g., ATS providers) pre-onboarding; include ISO 27001 Annex A.15 clauses in contracts (e.g., security audits, sub-processor notifications per UK GDPR Article 28).
- Share data only with authorisation; conduct periodic reviews.

Compliance and Auditing

- Appoint ISO and DPO to oversee ISMS and GDPR compliance.
- Bi-annual internal audits; annual external ISO 27001 certification audits; maintain records of measures (UK GDPR Article 24).
- Quarterly metrics reporting (e.g.training rates, incident times) to senior management.

Roles and Responsibilities

Role	Responsibilities
Senior Management	Approve Policy, allocate resources, review ISMS performance and risks annually.
Information Security Officer (ISO)	IMS Responsibility / Authority, Develop / enforce Policy, lead risk assessments, audits, and incident response, IMS Internal & External Communications, report to board.

Role	Responsibilities
Data Protection Officer (DPO)	Oversee GDPR compliance, handle DPIAs, subject requests, and breach notifications.
All Employees/Contractors	Adhere to Policy, report incidents, complete training.
IT Department	Implement controls, monitor systems, perform backups and scans.
HR/Recruitment Team	Integrate security in onboarding, manage consents and access reviews.

Training and Awareness

- Annual mandatory e-learning on security topics (e.g., GDPR obligations, phishing in recruitment contexts); quarterly simulations (e.g., phishing tests).
- Ongoing awareness via newsletters, posters (e.g., "Verify before sharing candidate details").
- Tailored to roles, ensuring 100% completion.

Monitoring, Review, and Enforcement

- Review Policy annually, or post-incident/regulatory changes (e.g., new UK guidance).
- Violations may lead to disciplinary action (up to termination) and law enforcement referral.
- Feedback to ISO/DPO at security@athona.com or dpo@athona.com

Approval and Version Control

Version: 2.0

Effective Date: March 2026

Next Review: March 2027

Owner: Information Security Officer (ISO)

Approved by: Senior Management / Board

Approval Signed: Stewart London (CEO / Board Chair) Date: Mar 2026