

Information Security Policy statement

At Advance TRS Ltd., we are committed to ensuring the privacy, security, and integrity of all personal and sensitive data that we retain. Our goal is to safeguard all forms of data while continually improving our information security management system (ISMS) to protect against emerging threats and comply with evolving regulatory requirements.

Information Security Objectives

We are dedicated to establishing, maintaining, and reviewing information security objectives. These objectives are focused on:

- **Safeguarding the confidentiality, integrity, and availability** of all personal, client, and organisational data.
- **Minimising unauthorised access** through robust access controls and multi-factor authentication.
- **Ensuring compliance** with all applicable laws, regulations, and contractual obligations related to information security, including GDPR, the Data Protection Act 2018, and any future legislation.

These objectives are reviewed annually or following significant incidents to ensure that they remain relevant and effective. We have established a structured framework for setting, implementing, and reviewing these objectives as part of our broader risk management and audit process in the IMS Planning Workbook.

Commitment to Compliance

Advance TRS Ltd. is fully committed to complying with all applicable legal, regulatory, and contractual requirements related to information security. This includes, but is not limited to, the **General Data Protection Regulation (GDPR)**, the **Data Protection Act 2018**, and other industry-specific standards where relevant.

We recognise the importance of adapting to **emerging legal requirements** and ensure that any changes in legislation are reflected in our information security practices and policies. Our compliance commitment includes regularly monitoring and updating our systems and procedures to address new or revised regulations.

Data Collection, Processing, and Storage

All personal data is collected, processed, and stored in line with the principles of transparency, fairness, and accountability:

- **Candidate Data:** Captured through the Advance TRS registration process, either digitally or verbally, with a clear explanation provided regarding why the data is collected and how it will be used. No personal data will be shared with third parties without the express consent of the individual.
- **Employee Data:** Collected during recruitment and induction, with the accuracy and completeness of the data regularly reviewed with the employee. Employee data is stored securely with dual authentication access controls and tiered permissions based on role

and responsibility.

- **Data Storage:** All personal data is stored in a password-protected database located on an external server within a high-security UK data Centre or in secure data folders with dual authentication. Or in our secure digital filing system, or HR software secured with multi-factor-authentication.

Commitment to Continual Improvement

- At Advance TRS, continual improvement is central to our approach to information security. We are committed to: **Conducting regular audits and business continuity testing** to assess the effectiveness of our security controls.
- **Ongoing risk assessment** and incident reporting to identify vulnerabilities and implement corrective actions.
- Integrating feedback from **client audits, supplier reviews, professional advisors/specialists or ISO27001 audits**.
- **Adopting technological advancements** and innovative practices to improve the resilience of our ISMS and prevent security breaches.

Risk Management and Incident Response

Risk management is an integral part of our ISMS. We identify and mitigate risks related to data security through:

- **Regular risk assessments** linked to our risk register.
- **Ongoing evaluation of threats** related to data breaches, cyberattacks, and unauthorised access.

In the event of a security breach, Advance TRS has a clear **business continuity and accident & incident procedure**. All breaches are logged, investigated, and, if necessary, reported to the **Information Commissioner's Office (ICO)** within the required timeframes. Breaches that may result in significant harm, such as financial loss or identity theft, will be escalated and communicated to the affected individuals.

Access Control and Data Security

Access to personal data is managed using **multi-factor authentication and role-based access control**. Only authorised personnel are permitted to access sensitive data, and permissions are reviewed regularly to ensure that access is limited to individuals who need it for legitimate business purposes.

We ensure that all systems are **monitored continuously** for potential security breaches or weaknesses. Any suspected vulnerabilities are addressed promptly to maintain the highest level of data protection.

Employee Training and Awareness

Advance TRS ensures that all employees receive regular **training on information security** and data protection principles. This ensures that employees understand their responsibilities and the importance of protecting personal and sensitive data. Training is provided as part of our

onboarding process and is refreshed periodically to reflect any changes in laws, regulations, or internal policies.

Transparency and Subject Rights

Advance TRS communicates openly with internal and external stakeholders on how personal data is collected, processed, and stored. We provide all individuals with:

- **The right to access their personal data** upon request, with all requests answered within 28 days.
- The option to **update or correct their data** at any time.
- The right to **complain to the ICO** if they believe their data has been mishandled.
- **The right to remove data** upon request, with all requests answered within 28 days.

All subject access requests will be provided in a clear, standardised format, and multiple requests over a 28- day period may incur a nominal administrative fee.

Consent and Data Integrity

Consent for the collection and processing of personal data is gathered through **unambiguous consent mechanisms**. We ensure that individuals provide a **positive indication of agreement**, rather than relying on assumptions of consent by default. Individuals have the option to withdraw their consent at any time.

Advance TRS regularly reviews the quality and accuracy of personal data held, offering routine opportunities for data updates. Ensuring data integrity is a priority, and we use data validation techniques and compliance monitoring to uphold this standard.

Andy Ridout



Managing Director

September 2026

