Crowe

Smart decisions. Lasting value.™

Information Security Statement

July 1, 2025

Information Security Statement

Crowe LLP is committed to maintaining confidentiality, integrity, and availability of personal data in compliance with applicable data protection laws, including the General Data Protection Regulation (GDPR), the UK Data Protection Act, and the EU-U.S., UK-U.S., and Swiss-U.S. Data Privacy Frameworks (DPF) where applicable. This Information Security Statement or Technical and Organizational Measures (TOMs) outline the security controls in place to safeguard personal data processed by Crowe LLP.

1. Organizational Measures

1.1 Data Protection Governance

- Appointed Chief Compliance and Privacy Officer (CCPO) to oversee compliance.
- Regular Privacy Impact Assessments (PIAs) for new projects involving personal data.
- Cross-functional Security and Privacy Committee to review and update data protection policies.

1.2 Policies and Procedures

- Data Protection Policy governing personal data processing.
- Access Control Policy implementing role-based access controls (RBAC).
- Data Retention and Deletion Policy supporting secure data disposal.
- Incident Response Plan for breach detection, reporting, and remediation.

1.3 Employee Training & Confidentiality

- Annual privacy and security training for all employees.
- Mandatory confidentiality agreements (NDAs) for employees and third parties.
- Ongoing security awareness initiatives, including phishing simulations, reinforce personnel vigilance and risk mitigation.

2. Technical Measures

2.1 Access Controls

- Physical Security: Key card access, smartphone-based access control, CCTV surveillance, and visitor logs.
- Logical Security: Multi-factor authentication (MFA) and least privilege access principles.
- User Activity Logging & Monitoring: Audit trails for data access and processing activities.

2.2 Data Encryption and Transmission

- Data at Rest: encryption for stored data.
- Data in Transit: encryption for secure communication.
- Encrypted backups stored securely offsite.

2.3 Network and Endpoint Security

- Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS).
- Endpoint Security: Antivirus, anti-malware, and endpoint detection response (EDR) solutions.
- Secure VPN access for remote employees.

2.4 Data Backup and Recovery

- Automated, encrypted backups are performed daily and stored securely.
- Business Continuity Plan (BCP) consisting of the Disaster Recovery Plan (DRP) and Incident Response Plan (IRP) are documented and maintained to confirm rapid restoration of critical systems.
- Backup integrity is verified through period testing.

3. Risk Assessment and Management

3.1 Risk Analysis

- Risk assessments are performed to identify, evaluate, and mitigate threats.
- Threat intelligence monitoring to address emerging cybersecurity risks.
- Risk register tracking and mitigation strategies.

3.2 Monitoring and Auditing

- Continuous security monitoring with Security Information and Event Management (SIEM) solutions.
- Regular internal and external security audits.
- Penetration testing conducted by certified security professionals.

4. Incident Response

4.1 Incident Management Plan

- Security Operations Center (SOC) monitoring for threats and suspicious activity.
- Incident containment and forensic analysis to determine root cause.
- Remediation and corrective actions to prevent recurrence.

4.2 Breach Notification

- Regulatory reporting requirements are met within required timeframes, including 72-hour deadline under GDPR requirements.
- Notification to affected individuals, as appropriate, with risk mitigation guidance.
- Post-incident review to strengthen future response measures.

5. Continuous Improvement

5.1 Policy and Procedure Reviews

- Annual review of security measures to address evolving threats and industry practices.
- Updates to policies based on regulatory changes and audit findings.

5.2 Employee and Stakeholder Feedback

- Internal reporting mechanism for employees to flag security concerns.
- Regular security communications to foster and encourage continuous learning and engagement.
- Client and third-party security reviews and assessments for vendor compliance.

6. Privacy Program

6.1 Privacy Compliance

- Records of Processing Activities (RoPA) maintained per GDPR requirements.
- Data Subject Rights Management System to handle access, rectification, and deletion requests.
- Privacy-by-Design principles embedded in all IT projects.
- Data minimization principles are applied, and the collection and processing of personal data are limited to what is necessary for the specified and legitimate purposes.

6.2 Data Transfers and Third-Party Management

- Standard Contractual Clauses (SCCs) are used for cross-border data transfers in accordance with applicable laws.
- Third-party vendors undergo security assessments before onboarding vendors and are subject to regular oversight.
- Binding Corporate Rules (BCRs), where applicable, for intra-group data transfers.

7. Contact Information

For further information regarding Crowe LLP's Information Security Statement or Technical and Organizational Measures, please contact:

Chief Compliance and Privacy Officer (CCPO)
Email: privacy@crowe.com