Schedule 1

Data Protocol

Types of personal data to be processed and categories of data subject

The provision of the Services will involve the Supplier processing Personal Data during the Term as described in more detail below:

List of Parties	**Data Controller: Client** **Data Processor:** Citation Cyber Ltd **Address**: Kings Court, Water Lane, Wilmslow, Cheshire, SK9 5AR. **Contact:** dpo@citation.co.uk
The subject matter of the processing	The personal data of the Data Controller's employees will be processed by the Data Processor in the delivery of the services.
The duration of the processing	The duration of the processing will match the main service agreement.
The nature and purpose of the processing	Citation Cyber will process personal data for the following purposes: • The provision of Cyber Awareness training. • The provision of Phishing simulator. • The provision of Cyber Essentials Certification. • The provision of Penetration testing and Simulated Hacking. • The provision of Intelligent scanning. • The provision of Professional Consultancy services. • The provision of Policy and document management.
The type of personal data being processed	Full Name Email Phone Number Address DOB Online identifiers Other data appropriate under the contract and data processing agreement determined at time to time.
The categories of data subjects	Employees (including, but not limited to, contractors, consultants etc.) of the data controller using the Citation Cyber products and services for their training purposes.

Technical and Organisational Security Measures

The following sections define our current technical and organisational measures. We may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

1. **Information Security Program and Organisation**
    1.1. We maintain and will continue to maintain a written Information Security Program that includes policies, procedures, and controls, including the Information Security Policy.
    1.2. The Information Security Program is maintained in accordance with ISO27001 standards.
    1.3. We will use external auditors to test and verify the adequacy of our Information Security Program and will maintain ISO 27001 certification.
    1.4. A dedicated team is responsible for the Information Security Program.
    1.5. We have appointed a DPO (Data Protection Officer).

2. **Human Resources and Security**
    2.1. We will conduct reasonable and appropriate background/verification checks on all staff prior to employment, including checks of identification, right to work and verification of previous employment. Enhance checks may also be conducted depending on job role.
    2.2. Our staff access to client data is bound by confidentiality clauses within their employment contract and non-disclosure agreements.
    2.3. We will conduct security awareness/cyber security training once per month and data protection training annually for all staff.
    2.4. We have formal disciplinary processes in place to take action against staff who breach internal Policies.

3. **Physical Security Controls**
    3.1. Our platform is hosted in Amazon Web Services (AWS) which have a defined and protected physical perimeter, strong physical controls including, but not limited to, access control mechanisms, tightly controlled outer and inner perimeters with increased security at each level, including perimeter fencing, security officer, locked server racks, integrated alarm systems, around the clock video surveillance, and multi-factor access controls. For further details please refer to AWS - https://aws.amazon.com/complaince/data-center/controls/
    3.2. We ensure that access to the Client facilities is tightly controlled through access control systems (e.g., smart card access system). All visitors to the Client premises must register at reception and are accompanied by authorised personnel at all times. Further additional measures include CCTV, and intruder alarm systems.

4. **Access Controls**
    4.1. We maintain a formal access control policy and employ a centralised access management system to control staff access to client data and to support the secure creation, amendment, and deletion of user accounts.
    4.2. We regularly review the access rights to ensure that all user accounts and user account privileges are allocated on a need-to-know basis. Upon a change in scope of employment or termination of employment, access rights are removed or modified as appropriate.
    4.3. Least privileged Role Based Access Controls (RBAC) are in place across our network.
    4.4. Access to highly sensitive systems and cloud infrastructure is controlled by secure log-on procedures including Multi-Factor Authentication or Virtual Private Networks.

5. **Operational System Security and Encryption**
    5.1. We maintain a formal Software Development Lifecycle Framework that includes secure coding practices based on Open Web Application Security Project (OWASP) recommendations and related standards and will perform both manual and automated code reviews before the code is released into a production environment.
    5.2. We perform an external penetration test of our client facing applications on an annual basis to assess the security of the service. All tests are undertaken by a CREST certified third-party.
    5.3. We maintain an isolated production environment that includes commercial-grade network management controls such as a load balancer, firewall, and intrusion detection system.
    5.4. We encrypt and protect all data in transit using TSL 1.2 or above for any communication between services or from client to server.
    5.5. We encrypt and protect all data at rest using Transparent Data Encryption (TDE) for SQL Databases. Storage data is encrypted by default using 256-bit AES encryption (FIPS 140-2 compliant).
    5.6. We run regular internal vulnerability scans utilising best in class third party applications. CVE scores are used when conducting vulnerability scans and known vulnerabilities are categorised and remediated.
    5.7. We have in place password requirements for internal users with a minimum 16-character passphrase consisting of 3 unconnected random words. For the client facing application the password requirements are 8-20 characters, at least one lowercase letter, one uppercase letter, one number and at least one special character (?!*@).
    5.8. We have firewalls and gateways on all internal networks and protection via proactive threat hunters.

6. **Incident Response and Breach Notification**
    6.1. We maintain procedures that ensure an appropriate response to security incidents addressing monitoring, investigation, response, and notification.

7. **Business Continuity and Disaster Recovery**
    7.1. We store client data redundantly at multiple locations in our hosting provider's data centres to ensure availability. We maintain backup and restoration procedures, which will allow recovery from a major disaster.
    7.2. We maintain a business continuity/disaster recovery plan. The plan provides for the restoration of access to client data, a continuation of operations and Services during a range of short-term and long-term disaster events. The plan covers re-establishment of information technology environment(s) following an unplanned event impacting the data centre, infrastructure, data, or systems.
    7.3. The Business continuity/disaster recovery plan and related procedures are tested at least annually.

Approved Processors

Amazon Web Services
Service – Cloud Infrastructure Provider – Where the application code and database reside. We also use Amazon S3 to store daily, weekly, and monthly backups of the database.
Location of Processing (Country) – UK
Cross-border Documentation in place – N/A

Microsoft Corporation
Service – Cloud Infrastructure Provider – Where the application code and database reside. We also use Microsoft to store daily, weekly, and monthly backups of the database. Office 365 – personal data included in emails, documents and other data transferred in electronic form in the context of using MS services.
Location of Processing (Country) – UK
Cross-border Documentation in place – N/A

Pipedrive
Service – Sales Management and CRM system.
Location of Processing (Country) – UK & USA
Cross-border Documentation in place – EU standard Contractual Clauses and UK Addendum along with TRA. UK Extension to the EU-US Data Privacy Framework

PandaDoc
Service – Document Creation and Electronic signatures.
Location of Processing (Country) – UK & USA
Cross-border Documentation in place – EU standard Contractual Clauses and UK Addendum along with TRA. UK Extension to the EU-US Data Privacy Framework

IASME
Service – Cyber Essentials Standard Governance Service.
Location of Processing (Country) – UK
Cross-border Documentation in place – N/A

Qualys
Service – Cloud based scanning service.
Location of Processing (Country) – UK
Cross-border Documentation in place – N/A

AppCheck

Service – Vulnerability Scanning provider.
Location of Processing (Country) – UK
Cross-border Documentation in place – N/A

Xero
Service – Accounting and invoicing service provider.
Location of Processing (Country) – UK & New Zealand
Cross-border Documentation in place – N/A

Vonage
Service – Contact Centre Telephony Software & Call Recording Cloud Communication provider.
Location of Processing (Country) – UK & USA
Cross-border Documentation in place – EU Standard Contractual Clauses, UK Addendum and TRA. UK Extension to the EU-US Data Privacy Framework

FreshService
Service – Client support ticketing.
Location of Processing (Country) – UK
Cross-border Documentation in place – N/A