Minerva Security Questionnaire

The purpose of this questionnaire is to answer questions relating to our services and provide a general overview of the security controls, data protection and risk management processes in place during the provision of our services to our customers.

1. Security Compliance and Policies

1.1	What security certifications do we currently hold?	We are Cyber Essentials certified while also working towards ISO 27001 standards.
1.2	Does the organisation have an Information Security Policy?	Yes, a documentation on our security information is provided here.
1.3	Has the organisation undergone any third-party audits or certifications?	We are currently working on this as part of our ISO 27001 project.
1.4	Do you have a Security Policy & Acceptable Use Policy in place which sets out the security measures to be implemented and followed in relation to the services provided to your clients?	There is an IT Policy that defines acceptable use and Information Security Policy which is signed off.
1.5	Do you have a suitable policy and controls that protects customers against unauthorised access, loss or disclosure arising from data stored on writable CD drives, memory sticks, other output devices or printed media?	Yes, we have an IT policy that protects against this.

2. Data Retention and Policy

2.1	How long is the data retention period?	Data is retained for a period of 7 years considering our data protection obligations, including to keep data for no longer than is necessary for the purposes for which it is processed, balanced against our business requirements to retain the data and the technical and organisational measures involved in deletion.
2.2	How is data processed or removed after this period?	Data is removed both from the Quote Portal and Client Portal.
2.3	Can clients request for data to be removed for requests relating to GDPR?	Yes, clients can request for data to be removed, and we'll get that processed within 30 days of request. Our Data Retention Policy can be found here.
2.4	Does the organisation process any PII data related to the services provided and how are they protected?	Yes, data provided by your clients in the portal is stored and encrypted in Azure SQL.

3. Security Awareness and Training

3.1	How do you handle phishing and social engineering awareness?	Our employees go through various training on spotting and detecting phishing emails and campaigns and additional training assigned in case of a user failing this.
3.2	Do your employees receive regular cybersecurity training?	Yes, and we are also currently updating our training materials as part of our ISO 27001 preparation.
3.3	Is there physical control to the office premises and controlled physical access to the machines and PCs in the office?	Yes, there is physical control to the office premises.

4. Network and Infrastructure Security

4.1	Do you use firewalls, IDS/IPS, or other network security tools?	Our Minerva software is protected by both internal and external threats as we utilize Web Application Firewall in Azure for our web applications and Defender for Cloud also in use for our cloud resources.
4.2	How do you monitor for suspicious activity or breaches?	Suspicious activities and breaches are monitored with Microsoft Defender for the cloud alongside Azure tools which are designed for this.
4.3	What endpoint security measures do you have in place?	We make use of Microsoft Defender XDR for our endpoint security.
4.4	Do you ensure that your network infrastructure is protected and segregated from the public?	Yes, our network is segregated and is only connected to MS Azure, and we have SonicWALL in place at our office location

5. Data Protection and Encryption

5.1	How is data encrypted while at rest and in transit?	All communications are encrypted via SSL and the data is encrypted at rest
5.2	How do you handle and store customer data?	All customer data is stored in the Azure Cloud systems in compliance with GDPR rules
5.3	Are there controls in place for access to the data to identify, protect and preserve data and records?	Yes, there are RBAC rules and least privilege enforced for access to data and systems.

5.4	Is there segregation of data to protect them being shared with or accessed by other customers for cases not relating to them?	Yes, segregation is available at the tenant level to avoid cross-tenant data leak.
5.5	Is there a dedicated staff overseeing data security such as Data Protection Officer or Chief Information Security Officer	Gareth Jones (Senior Technology Consultant) and Mark Hemmings (Operations Director)

6. Vulnerability and Patch Management

6.1	How are vulnerabilities and security patches managed?	Automatic updates are enabled on all client machines as we follow NCSC/Cyber Essentials guidelines on patching.
6.2	Do you conduct penetration testing and vulnerability scanning of the systems?	We conduct penetration testing to identify and amend vulnerabilities found in the web application
6.3	Are there results of the penetration testing?	Our latest results are available here.
6.4	Are changes made to the environment, supporting architecture or systems carried out and authorized via Change Management Process?	Yes, all changes to be made are reviewed and authorized.

7. Access Control and Authentication

7.1	How are user access and permissions managed?	Access to the system is controlled by using a RBAC system wherever possible as well as least privilege policy to control access to different features of the system for people who don't require access to them.
7.2	What authentication methods are used on the system?	MFA and SSO is also available for system access. For our Minerva Quoting/Referral system, email MFA is supported and for the Minerva Client Portal, email MFA, SMS MFA and Authenticator MFA is supported for gaining access to the portal.
7.3	Are there password policies enforced for our employees?	Yes, there is an IT policy that covers password policy.
7.4	Is there a policy in place to ensure that staff lock their workstations when they are unattended OR is there a timed screen lockout out after a period of inactivity?	Yes, there is a Group Policy in place to effect screen lockout after a period of inactivity.

7.5	Is there a process of user and password creation to ensure users have unique accounts and are issued to users in a secure manner?	Unique links are sent to users when creating accounts for the Minerva referral system and client portal.
7.6	Is there an account lockout process for users trying to log into the system after multiple failed attempts or incorrect password?	Yes, users are locked out for a period after incorrect password attempts on both the Minerva referral system and client portal.

8. Business Continuity and Incident Response

8.1	Are critical information records adequately protected and duplicated/backed up in secure, off-site locations?	Yes, data is protected and backed up in Azure cloud.
8.2	What Business Continuity and Disaster Recovery plans are in place?	The Minerva system is situated in the Azure Cloud with backups in different regions to accommodate for our Business Continuity and Disaster Recovery systems.
8.3	How quickly do we notify customers in case of a security breach?	In cases of a breach or an incident, we have appropriate business continuity strategies in place which caters for how to recover data and keeping our clients informed if needed once the severity of incident has been determined.
8.4	Are continuity plans for critical processes and activities updated and reviewed annually?	Yes, this is reviewed but currently undergoing our ISO 27001 project so this review process will be continued in the future.
8.5	Is there an adequate disaster recovery process or accommodation for personnel/staffs to work remotely in case of the onsite premises being unavailable?	Yes, all staffs can work remotely should the office be unavailable.

9. Third Party and Supply Chain Security

9.1	Are there third-party or subcontractors that data are shared with?	A list of our 3rd party sub-contractors is available in the Data Processing Policy available here.

9.2	How do you manage third-party risk?	We are enhancing our Third Part Risk Management as part of our ISO 27001 and will be reviewing our suppliers as part of this process.
9.3	Are all sub-contracted or third-party services (including SaaS, PaaS, IaaS) subject to appropriate suitability assessments to ensure their data security is equal to or better than your own and appropriate to your customers' needs and potential regulatory requirements?	Our third-party security and security policies are all reviewed and as part of our ISO 27001 policy preparation.

10. Coding, Development and Software Security

10.1	Do you follow secure coding practices?	Our developers follow a very secure SDLC approach to development for our web applications. All updates and changes to be made are tested in a secure test environment before applying to the live system.
10.2	How do you test for security vulnerabilities in your software?	All our third-party tools are regularly tested for known vulnerabilities as well as penetration testing carried out on our system as well.
10.3	Are production services logically segregated from development and test environments with access control & segregation of duties enforced?	Yes, our test environment is segregated from the production environment.

11. Compliance and Legal Considerations (Insurance)

11.1	Is there cybersecurity insurance in place?	There is cyber liability insurance in place for our risk transference strategy. All insurances can be found here: https://www.minervaportal.com/minerva-terms-requirements/insurances
11.2	Can you provide evidence of compliance with legal and regulatory requirements?	We follow legal and regulatory requirements as required by the policies we follow here at Minerva alongside Cyber Essentials and ISO 27001.
11.3	Do all third-party service providers have suitable cyber insurance in place?	Yes.

12. Onboarding, Offboarding and Termination

12.1	How long after termination do you retain data before permanent deletion?	We follow our Data Retention Policy for clients no longer with us unless otherwise required based on requests which will then be discussed.
12.2	How is data securely deleted or returned upon contract termination?	Data is securely deleted from both referral system and client portal system.
12.3	Do you have procedures to ensure the removal of your organisation's and/or customer data from systems sent for disposal?	We have offboarding procedures depending on the termination type.
12.4	Do you conduct screening and checks on all new employees, including those without direct access to systems containing customer data (e.g. administration or cleaning staff)	We carry out a Right To Work, Credas ID checks.
12.5	Are onboarding processes in place for new staffs?	Yes, there is a process to onboard new staffs.
12.6	What controls are there for end users accessing the system?	There are MFA controls in place for end users accessing our system.