Information Security Questionnaire for all centralised services provided by Chambers

This questionnaire has been agreed by the Law Society and Bar Council. It was devised by a joint Law Society / Bar Council working group representing the interests of barristers' Chambers and a number of larger law firms in 2021 and was subjected to wider review in various roundtable discussions in early 2022. It comprises a standardised questionnaire the purpose of which is to enable law firms to better assess the information security arrangements of the Chambers whose barrister members they instruct. The questionnaire has been compiled with brevity and simplicity in mind. It is hoped that by having an agreed standardised questionnaire the administrative burden will be much reduced for both the Chambers responding to the questionnaire and the law firms assessing those responses.

The questions are intended to be relevant for most circumstances. The Law Society and the Bar Council recommend their use. In drafting this questionnaire, the joint Law Society / Bar Council working group has been mindful of problems associated with inappropriate and/or irrelevant questions being asked of barristers' chambers. For that reason, we recommend you avoid supplementary questions where possible, or separate them from the primary questionnaire. Further or different questions may be appropriate in specific cases.

Answers to the questionnaire do not necessarily imply compliance with established frameworks such as ISO27001, NIST and Cyber Essentials, to which reference can be made as necessary by those Chambers wishing to align their security programmes to an acknowledged information/cyber security standard.

Because most barristers are self-employed, independent practitioners, and given the variety of ways in which their Chambers are set up, the questionnaire focuses only on central systems and services which may be provided by Chambers to barristers and staff. Individually owned and managed devices, and information technology (IT) services procured directly by barrister members fall outside the scope of this questionnaire. This is because barristers have their own data protection duties and obligations, which they are compelled to observe by their regulator, the Bar Standards Board, and by law. Though this is of paramount importance, the aim of this questionnaire is to ensure that Chambers are information security compliant and to promote a culture of change across the legal profession in terms of how law firms instruct barristers. The questionnaire therefore begins by seeking a definition of the scope of such centrally provided systems and services. The remaining questions should then be answered in respect of that defined scope.

We recommend that Chambers work with their IT suppliers and maintain an up-to-date copy of their responses to this questionnaire which they can make available to instructing solicitors with the aim of revisiting them every six months.

The answers to this questionnaire are confidential and are not to be provided to any other party without express written consent from Chambers.

Scope of central Chambers' services

1. Does Chambers provide any central IT infrastructure systems and services? If "*Yes*", please detail: (a) that system/service; and (b) to whom each system / service is provided.

Central IT infrastructure systems/services	"Yes" or "No"	Systems/Service detail (e.g., Email – Office 365)	To whom that system/service is provided (e.g., individual Barristers and/or Chambers Staff)	Is the system/service on-premises, privately hosted or cloud based?
Email				
Diary, practice and fees management (e.g., Lex, MLC, other)				
Document Management (or other document storage) system				
Other (e.g., file sharing)				

Risk Management

2. Is Chambers certified or aligned to any acknowledged security frameworks (e.g., ISO27001, Cyber Essentials, Cyber Essentials Plus)? If "Yes", please detail and provide copies of the Certification and Statement of Applicability.

Yes

3. Has Chambers identified its main operational risks, ensured its information security processes seek to mitigate these risks, and will the Management Committee, Head of Chambers or similar review/approve these, every six months?

Yes

4. Does Chambers have arrangements for ensuring security of its premises, including (but not solely) a formal procedure for handling visitors/sub-contractors working on premises?

Yes

Engagement & Training

5. Does Chambers provide mandatory information security awareness training for Chambers' Staff, which is refreshed annually?

Yes

6. Does Chambers make annual information security awareness training available to individual Barristers, or encourage Barristers to attend annual information security awareness training?

Yes

Asset Management

7. Does Chambers have an information asset register/data map to keep track of:
   - the information it processes; and
   - where that information is located?

Yes

8. Does Chambers have documented policies and procedures concerning the storage, retention and destruction arrangements for all client information?

Yes

9. Is any instructing law firm and/or lay client information stored by or on behalf of Chambers outside of the UK and/or the EEA (e.g. in cloud servers not located in the UK or in the member states of the EEA)?

Yes

Architecture & Configuration

10. Does Chambers have regularly tested security mechanisms which are adequate to protect the physical and electronic security of its IT infrastructure and information (e.g., firewalls, web filtering, anti-virus and other products that scan for threats and viruses)?

Yes

11. Are back-up and restoration procedures for client and operational data documented and regularly tested?

Yes

Vulnerability Management

12. Does Chambers conduct vulnerability scans such as phishing and spam tests at least twice a year and penetration tests of its IT infrastructure at least once a year?

Yes

13. Does Chambers apply security patches as soon as possible or at least monthly?

Yes

Identity & Access Management

14. Does Chambers carry out personnel screening for employees (e.g., reference checks, relevant background checks)?

Yes

15. Are all Chambers' staff and individual Barristers assigned individual accounts to log onto central Chambers IT systems?

Yes

16. Does Chambers enforce the use of multi-factor authentication (MFA) for all remote connections to its IT infrastructure?

Yes

17. Does Chambers enforce the use of MFA for all connections to cloud-based systems?

Yes

18. Does Chambers enforce a password policy that is in line with recognised good practice?

Yes

19. Does Chambers have documented procedures for granting access to central Chambers' IT systems and services and to terminate access on or before a leaver's termination date?

Yes

Data Security

20. Is all remote access to central Chambers' IT systems/services appropriately secured (e.g., virtual private network (VPN))?

Yes

21. Are instructing law firm and lay client data on central Chambers' PCs and laptops encrypted at rest (within the central IT infrastructure) and (where possible) in transit (e.g., compulsory VPN connections to cloud and office-based services, TLSencryption for email)?

Yes

Logging & Monitoring

22. Are logs maintained which will support security incident investigations, and are they protected against modification, deletion and unauthorised access?

Yes

Incident Management

23. Does Chambers have an incident management process that is regularly reviewed and tested which details the steps it would take to respond to and recover from a cyber and/or information security breach?

Yes

24. Does Chambers maintain an incident register that logs both actual breaches and near misses (even if they do not need to be reported to regulators or individuals)?

Yes

25. Has Chambers experienced a significant data breach that has necessitated a report to a regulator (e.g., BSB, ICO) in the past 12 months? If "Yes", please provide details.

Yes

Supplier Security

26. Does Chambers conduct due diligence on its suppliers to ensure that appropriate and proportionate information security and privacy controls are maintained on an ongoing basis?

Yes

Glossary

Multi-factor authentication (MFA)

- Accessing an online account using multiple elements to prove the users' identity. Upon the first 'factor' being successfully entered, the user is then prompted to enter the second 'factor'. Two factors are the most common, but there may be more. The process is also known as 'two-step verification'. A factor can be: 1) something you know (e.g., password), 2) something you have (e.g., authentication token), 3) something you are (e.g., fingerprint).

International Organization for Standardization (ISO)

- A non-governmental organisation which sets standards in various fields that are recognised internationally by both commercial organisations and governments. ISO 27001, sets out the specification for an information security management system: https://www.iso.org/isoiec-27001-information-security.html

National Institute of Standards and Technology (NIST)

- A non-regulatory US government agency whose responsibilities include the development and publication of standards, including security standards, to drive innovation and competitiveness of US companies. NIST security standards are commonly adopted (including in the UK) in those sectors requiring the most stringent security controls, such as banking: https://www.nist.gov/

Cyber Essentials (PLUS)

- A UK Government-backed scheme designed to help organisations in implementing the required security controls to protect against cyberattacks: https://www.ncsc.gov.uk/cyberessentials/overview.

Virtual Private Network (VPN)

- A private and encrypted network connection that can be used to secure electronic communications over public Internet.