Secure23

KEEPING YOUR VENDORS HONEST

The below questions are based on the CIA triad; the internationally recognised model that defines the three core objectives of information security. It stands for Confidentiality, Integrity, and Availability. Asking these questions (and analysing the answers!) will help to give you confidence that your technology vendors are protecting your data and reducing your exposure to risk.

CONFIDENTIALITY
INTEGRITY
CIA TRIAD
AVAILABILITY

Confidentiality

Information should only be accessible to those who are authorised to see it.

1. Where geographically is the data stored?
2. Will you allow a review of a recent third-party audit?
3. Are you able to share the results of a recent penetration test?
4. Do you perform regular tests of security processes and controls?
5. Is multi-factor authentication (MFA)
    a. Available
    b. Enforced
    c. Not available
6. Do you currently have a patch and vulnerability management process?
7. Do you have a service that logs and monitors all logical access to customer data?

Integrity

Information should be accurate, complete, and protected from unauthorised modification.

8. Do you provide data backup services?
9. How are data backup and archiving services provided?
10. Do you regularly perform test restores?

Availability

Systems and data should be accessible to authorised users when they need them.

11. Does the SLA include a minimum availability over a clearly defined period?
12. Do you utilise technologies that protect against DDoS attacks?
13. Do you have business continuity and disaster recovery plans?
14. Do you formally test your business continuity and disaster recovery plans?

Incident Response

15. Do you have a formal incident response and management plan?
16. Do you test and refine the incident response and management process on a regular basis?