Seigur Limited CYBER SECURITY OVERVIEW

SUMMARY
Seigur Limited ("Seigur") provides IT Legal and Cyber Security services to both private and public sector organisations. The objective of the Cyber Security Overview is to summarise the industry-recognised security controls Seigur uses to maintain the confidentiality, integrity and availability of data, computing devices and services within Seigur's control. Seigur bases its security programme and controls around the NIST SP 800-53 series (NIST SP 800-53) and NCSC's cyber security guidelines (NCSC). Seigur's security controls apply to all Seigur employees and computing equipment, and cover all data held, used or transmitted by Seigur.

PEOPLE
Seigur employees are assigned unique credentials for access to computing devices and services. Security of the user authentication controls (passwords and secure tokens) are aligned with the complexity requirements as defined in NIST SP 800-53. Seigur employees maintain an active awareness of data protection requirements and the latest cyber security threats, risks and attack techniques in order to protect Seigur's computer systems and the data within its control. All access credentials and authentication logs across Seigur's systems are reviewed periodically.

DATA
Data is stored on Seigur's computer systems in a manner consistent with its security classification. For example, by using encryption at the hard drive level with additional encryption at file level for highly confidential information. Only authorised users are permitted to access data on a 'need to know' basis. All data storage devices (computers, hard drives and backup media) are encrypted to at least a minimum key strength as defined in NIST SP 800-53. Data is deleted at the appropriate time in line with the secure data destruction controls detailed in NIST SP 800-53 (this includes the secure destruction of physical media). Storage of data on un-encrypted media is prohibited. Data is frequently backed-up onto local data storage devices and stored in an encrypted format. When sharing confidential files with third parties Seigur employees are required to ensure that the file is sent via a secure method appropriate to the risk such as; 1) encrypting the file if sending via email (with the password sent via an alternative communication method), or 2) use Seigur's file sharing portal, or 3) use a secure file sharing portal provided by the client. For physical copies of data, Seigur operates a clear desk policy and securely disposes of paperwork via a cross-cut shredder.

DEVICES
All Seigur computing devices (laptops and mobiles) have full hard disk encryption enabled and are security hardened in line with NCSC guidance. Only authorised users have access to the computing devices. All operating systems and software are vendor supported and patched within the timescales defined in NIST SP 800-53, where available all applications and operating systems are set to auto-update. All Seigur computing devices have anti-malware software installed and configured in line with vendor guidance. Security logging and auditing are enabled on all computing devices and any alerts generated are responded to accordingly. Computing devices have all data removed as per the security controls defined in NIST SP 800-53 before disposal. Physical computing devices (laptops and backup storage media) are mainly located on Seigur's premises, however Seigur employees do occasionally travel to client premises. When travelling all Seigur's employees are required to never leave a laptop unattended. In the event of a stolen laptop the installed security software allows Seigur to remotely locate the laptop and delete the data stored on the computer. Additionally the laptop is set to delete the data stored on the disk after a small number of incorrect password attempts.

CLOUD SYSTEMS
Seigur uses business cloud providers for email and web hosting services and are configured by Seigur in line with the NCSC guidance. For email and web hosting services Seigur's business hosting provider is located within the UK and all data within such services is stored in UK data centres. The UK data centres have 24/7 security guards, 24/7 network monitoring and video surveillance in operation. To maintain availability of Seigur's email and web hosting services, UPS battery backup and on-site generators are configured and available.

TELECOMMUNICATIONS
Seigur's computer devices are located on firewall-protected company network. In addition, all laptops have a local software-based firewall installed and have security features configured in line with vendor guidance. The use of non-Seigur devices on the company network is prohibited. When away from the company network (e.g. using client, airport or hotel Wi-Fi), all Seigur laptops are configured to use the installed secure VPN client to maintain the confidentiality and integrity of the communications. The use of non-Seigur Wi-Fi access points without the VPN enabled is prohibited.