Frequently Asked Questions

PRIVACY

Is my client's password to their financial accounts stored in RightCapital?
No, we do not save your client's credentials. We partner with Envestnet | Yodlee to provide account aggregation. All of your client's banking credentials are managed by Envestnet | Yodlee, and we do not store those credentials. We communicate with Yodlee via an encrypted data link.

Will you sell my client's data to a third party?
No, RightCapital will not sell any data to a third party.

DATA SECURITY

Does any data provided by subscribers or end-users leave the United States of America?
No, all data is stored at ISO 27001 and FISMA-certified data centers managed by Amazon within the United States of America.

Do you use a PCI-compliant processor?
Specifically for credit card payments, we use PCI-compliant payment processor Stripe for encrypting and processing payments.

Do you offer a two-factor authentication for user logins to the RightCapital software?
Yes, RightCapital knows security is a critical component of your success. Subscribers can turn on the two-factor authentication feature for themselves and their clients

Does RightCapital utilize any encryption techniques for data in transit or data at rest?
All data in transit, including transmission between a user's computer and our servers are encrypted, using industry-standard HTTPS protocol. Our SSL certificate uses 2048-bit asymmetric and 256-bit symmetric encryption.
We use HTTPS Strict Transport Security (HSTS) to ensure only secure connections can be used for our website. Our website is accepted by and built into Google Chrome, Safari, IE 11, Edge and Firefox for this purpose.
Our servers take advantage of Perfect Forward Secrecy (PSF) to protect data transmission for modern web browsers. With forward secrecy, all past communication confidentiality is maintained even when a long-term secret key is compromised.
Data at rest, including name, email address, physical address, and uploaded documents – is encrypted when we store it. Such data is encrypted using AES-256.

Describe the physical security in place to control access to subscriber and end-user data at the hosted data center.
RightCapital's physical infrastructure is hosted and managed within Amazon's secure data centers and utilizes the Amazon Web Service (AWS) technology. Our data centers are hosted on both the east and west coasts of the US.
For additional information see: AWS Cloud Security

Describe your policy on granting logical and physical access to systems.
Access shall be granted based upon the principles of need–to–know, least privilege, and separation of duties. Access not explicitly permitted shall be denied by default. Access is reviewed quarterly and removed immediately upon termination.

Why types of network security techniques are utilized?
Firewalls, DDOS Mitigation, Spoofing and Sniffing protection and Port Scanning have all been implemented. Firewalls are utilized to restrict access to systems from external networks and between systems internally. By default, all access is denied and only explicitly allowed ports and protocols are allowed based on business need. Each system is assigned to a firewall security group based on the system's function. Security groups restrict access to only the ports and protocols required for a system's specific function to mitigate risk.
Host-based firewalls restrict customer applications from establishing local host connections over the loopback network interface to further isolate customer applications. Host-based firewalls also provide the ability to further limit inbound and outbound connections as needed.
Our infrastructure provides DDoS mitigation techniques including TCP Syn cookies and connection rate limiting in addition to maintaining multiple backbone connections and internal bandwidth capacity that exceeds the Internet carrier-supplied bandwidth. We work closely with our providers to quickly respond to events and enable advanced DDoS mitigation controls when needed.
Managed firewalls prevent IP, MAC, and ARP spoofing on the network and between virtual hosts to ensure spoofing is not possible. Packet sniffing is prevented by infrastructure including the hypervisor which will not deliver traffic to an interface which it is not addressed to. RightCapital utilizes application isolation, operating system restrictions, and encrypted connections to further ensure risk is mitigated at all levels.
Port scanning is prohibited, and every reported instance is investigated by our infrastructure provider. When port scans are detected, they are stopped, and access is blocked.

Do you perform regular reviews of user access rights? How often is the review performed?
Quarterly user access reviews are performed on an on-going basis. Access is immediately removed for employees no longer at RightCapital.

Describe how you safely dispose of media and assets that contain sensitive information.
All paper contains sensitive information that is no longer needed must be shredded before being disposed. No removable media is allowed by the Company. All equipment to be disposed of will be wiped of all data, and all settings and configurations will be reset to factory defaults.

EMPLOYEE RISK MITIGATION

Do you perform information security training for all employees?

Yes, all workforce members shall receive appropriate training concerning Company's security policies and procedures. Such Training will be provided on an ongoing basis to all new employees. Such training shall be repeated annually for all employees.

How do I know my data is safe with your employees?
All workforce members must pass a background check. Also, a condition of employment is to sign a confidentiality agreement.

AUDIT

Is RightCapital SOC II compliant?
Yes, RightCapital is SOC II compliant. Our most recent testing period covered July 1, 2022 through June 30, 2023 with a final report dated September 30, 2023.

There have been no changes to the network, systems, or overall processes since the last SOC II Audit.

Can we trust RightCapital's network set up?
RightCapital contracts with a reputable security vendor to perform a comprehensive external network penetration test and vulnerability assessment of all in-scope systems.
The last completed test was in March of 2023. Compared to other organizations assessed by Cerberus Cyber Sentinel Corporation, the RightCapital environment tested in March of 2023 was deemed to have a low exposure level from an external perspective. Overall, the testing indicated that there was no unauthorized access to systems or data in the target systems.
There have been no changes to the network, systems, or overall processes since the last penetration and vulnerability scan.

INSURANCE

Do you have adequate cybersecurity and business insurance coverage?
Yes, we currently carry cyber insurance coverage against potential risk. Our current coverage is $1mm+, as of the effective date of this document. We continue to evaluate our coverage on an annual basis, or more frequently should our business model have any material changes.