

SECURITY OF DEBTLOGIC HOSTED ENVIRONMENT

DebtLogic customers know their data is safe and secure. They never have to worry about security. Instead they focus their time and energy on their core business.

LOGICAL ACCESS

System engineers and developers access the hosted environment via Virtual Private Networks, or VPNs. Access is granted once they have provided the necessary dual-factor authentication. Every system within the hosted environment is protected with a password that changes on a regular basis and is known only to that user.

PHYSICAL ACCESS

Both the hosted software and all client data are housed in a world class, SAS 70-Type II certified, data center, monitored 24 x 7 x 365.

Physical security controls include:

- Multi-factor security infrastructure
- All access / egress points to the facility are alarmed
- Network operations behind bullet-proof glass
- Biometric scanners
- Video surveillance of core data center infrastructure and data rooms
- Hourly rounds performed to physically check NOC/Data Center status
- Individual combinations for equipment cabinets

VULNERABILITY MANAGEMENT

The hosted environment is secured with leading anti-malware protection, as well as multi-tier intrusion detection and prevention systems.

Servers perform on-access and daily active scanning for vulnerabilities and report all information to a central console.

Anything irregular is emailed to our systems engineer team for analysis. Regular external scans are performed to ensure the proper operation and configuration of perimeter controls.

Patches and updates to server operating systems, applications, and other systems are performed on a regular basis after proper testing.

Overall reports that cover vulnerabilities, patches, and attacks are reviewed by our engineers and security team on a biweekly basis.

SECURITY POLICIES AND PROCEDURES

Employees who interact with the hosted environment are assigned set roles that provide a separation of duties within the systems. This inhibits any one person from becoming a security risk.

For example, a database administrator may be able to view the database and export data from it. However, that same person cannot decrypt that

data to view it and move it off of the server. This is achieved through the use of security groups, and properly assigning user account to these groups in a way that prevents overlap of duties.

In addition, for certain cases, we use specific technologies that only allow our staff to access applications necessary to their roles.

DISASTER RECOVERY

The data within the hosted environment is backed up daily.

The data will be moved to a remote failover site, in accordance with agreed service levels.

To minimize downtime for individual

server loss, we use an “active/passive”, or N+1, design. If a server becomes unresponsive, the passive system is brought online to replace the previously active server. Once the downed server is repaired, it is tested offline and then becomes the passive server.



Please let us know if you have questions regarding the security of our hosted environments or if you'd like to review our full disaster recovery plan. We offer full hosting services which enable our clients to focus on credit counseling. However, if you prefer, we can also provide the software for implementation in your secure environment.