IT Data Security And Data Retention Policies Summary

DATA SECURITY

Access Controls

Physical access to datacenter is limited to personnel who require access for job function. Personnel are required to record the purpose for entering the cold room. Access logs from our lock system for the datacenter are reviewed monthly.

Access to servers and data is limited to personnel who require access for job function. Access requests are reviewed by business owners before access is granted. Privileged accounts are reviewed quarterly and all accounts are reviewed annually by business owners.

User passwords are controlled by a domain policy that enforces password complexity, expiration, and account lock-out for repeated failed login attempts. User login failures are logged and reviewed.

Separation of Duties

Development environments are separated from testing and production environments. Developers do not have access to production environments and any changes applied to the production environment are reviewed by the business owner.

Reverse Proxy

All hosted solution servers are behind a reverse proxy.

Network Separation

The network used by our hosted solution servers is separate from our internal network. Access to the hosted solution network is limited to authorized personnel and requires two factor authentication.

Encryption

Transmission of information can be encrypted if SSL option is enabled. All tape backups are encrypted.

Change Management

Change requests must be recorded and approved by business owners. Approved changes are applied by separate personnel from those requesting changes. Any required outages must be approved by business owners.

Application Vulnerability Scanning
All applications are scanned with IBM AppScan prior to being pushed to the production environment and when any subsequent changes are applied. All vulnerabilities classified above approved threshold are remediated prior to release.

Additional scans of the production environment take place every 6 months.

The application scans include but are not limited to the following vulnerabilities:
- Authentication bypass using SQL injection
- Blind SQL injection
- Cross-site scripting
- Unencrypted login request
- Password parameter in query
- Cross-site request forgery
- Inadequate account lockout
- Login error messages credential enumeration
- Browser exploit against SSL/TLS
- Session identifier not updated

Server Vulnerability Scanning
All servers are scanned using Qualys for vulnerabilities on a monthly basis. Remediation takes place monthly.
The server scans include checking vulnerabilities related to but not limited to the following:
- Missing OS patches
- Unnecessary open ports
- OS user account password policy non-compliance
- SSL Certificates
- Cross-site scripting
- IIS authentication
- Remote code execution

DATA RETENTION

Customer-provided user import files are deleted after two weeks once a successful import has been completed.

The customer application database will be deleted within 6 months of the site expiration, unless other factors require additional time before the deletion is completed.

After a customer database has been deleted, the database backups will remain in our backup system for up to one year