Handling of Customer Information

Customer database information should be stored in the Leading2Lean data center environment and should not be stored on Leading2Lean Employee laptops except for the following limited circumstances:

- The employee is onsite at a customer facility for installation, consulting, or other business,
- The customer has given Leading2Lean extended permission to use their data for development, testing, or marketing purposes,
- Or the employee is working on an open bug/issue that requires a local copy of the customer database. Customer data must be removed immediately following the resolution of the issue.

Risk Assessment and Management

Vulnerability scanning and risk assessments should be performed at least quarterly. Results are to be presented to Leading2Lean management for review and for further action. Based on the results, independent testing and audits may be initiated.

Data Classification, Integrity, & Confidentiality

Access to data stored in Leading2Lean system shall be protected by individual username and password. By default all customer data is deemed confidential and will be treated as such. Data integrity shall be maintained through application controls at the application and database layers. Customer backups will under go periodic restores to ensure the integrity and usability of the data. Customer data being used outside of the Leading2Lean data center environment in the use cases listed above, should be encrypted if requested by the customer.

For more information see our Data Classification Policy.

Employee Security Training

All Leading2Lean employees must review the company security procedures upon hire and annually. Employee training will be tracked and documented.

Access & Authentication

- All Leading2Lean employees must be both qualified and vetted and before being granted access to computer systems and data.
- Employee should be given the least applicable privileges needed to accomplish their assigned tasks.
- Passwords should be forced to change on a periodic basis with reuse prohibited.

Production Service & Physical Data Center Security

Security in the Leading2Lean production data center environment is critical to our success. The following security production security policies must be observed.

1. All production databases must be backed up on a daily basis in a secure manner.
2. Backups must be test restored on a periodic basis.
3. All production servers must be secure with individual user names and passwords with IP address banning on multiple failed log in attempts.
4. Only production-qualified employees with applicable job assignments will be given access to the production environment.
5. Security patches will be tested, implemented, and monitored to ensure production stability and security.
6. Change management and testing procedures will be followed.
7. Customer data will be segregated to ensure confidentiality.
8. Firewalls will be used at the network and server levels.
9. Security alerts will be monitored and responded to 7x24x365 with formal incident response produces followed in the event of an incident.