**Technical Solutions**

**Classic-Tyler Motors, Inc. / Classic-Tyler Motors II, Inc. dba**

**Classic Toyota / Mercedes-Benz of Tyler**

1. Encryption:

All information received via company-handle email is encrypted.

PII gathered from customers for use in retail sales is to travel through the specific channel of portal@myclassictoyota.com or portal@myclassicmb.com. These email addresses distribute to Finance Managers’ company email addresses.

PII gathered from customers for use in vehicle purchases is to travel through the specific channel of UCD@myclassictoyota.com. This email address distributes to Used Car Sales Managers’ company email addresses.

Only the dealership Systems Administrator has direct access to any of the email addresses that have been created for the sole purpose of receiving PII.

Absolutely no PII is to be collected or stored on cell phones, iPads, or desk PCs. It shall be loaded directly to the dealership DMS and then deleted.

Bit Locker is installed on select employees computers that contain confidential or restricted information: (i.e. HR, Controller, Office Manager) Encryption keys are stored in IT Glue.

All Lexmark printers have TLS encryption. We currently have two Ricoh printers/copiers that do not have TLS encryption. Ubeo is working on getting us a certificate to install on those devices. Until certificate is available, the Ricoh devices shall not be used for gathering restricted information.

1. Access Controls:

Only the dealership Controller has authority to grant permissions to restricted information. Employees may request permissions directly from the Controller or through their department manager.

Controller has been added as a user on the IT Help Desk to ensure faster response times in granting and updating permissions and for documentation purposes.

Department managers may request access for vendors, in which case their data security policies will be requested. Controller will work with the Systems Administrator to determine if permission should be granted or denied.

Fortigate firewalls are in place and updated as needed to ensure network security: that all bugs and known issues are patched as computers access the internet.

Servers are secured, either in locked rooms or on locked racks.

1. Multi-Factor Authentication:

Multi-Factor Authentication will be required on all employees’ email accounts, Wildix logins, Slack, and Tekion logins. Additionally, MFA will be required at the Windows level, through Duo, for select members’ of management who have a high level of access to restricted information.

1. Testing will be performed to verify the security of of internal and external applications that are used to handle and store confidential and restricted information. Penetration testing will be performed internally twice yearly, and externally annually. Third-party vendors who have access to secure systems will by analyzed by the IT Director. Vendors who return deficient results will be required to upgrade security measures, or it will be determined to discontinue utilization of their services.
2. Secure Data Destruction: Retired equipment will be wiped out or drives removed by IT Department. We will send items periodically to Anything IT for sanitization services.
3. Change Management: Request shall be made to the CISO via email or written communication for approval to change or add hardware, software, applications, or third-party vendors. Once authorized, the IT department will make the necessary changes.
4. Information System Monitoring and Periodic Review: Monitoring logs shall be forwarded to Nuspire for analyzation. Any security vulnerabilities are to be reported by Nuspire directly to the IT Director.

External vulnerability scanning will be performed using SecureWorks VDR each quarter.

Internal penetration testing will be performed twice yearly through SecureWorks.