Data Protection and Information Security Requirements

Asset Management	
SEC-AM-1	Supplier will implement mechanisms to maintain an accurate inventory of assets and establish ownership and stewardship of all assets.
SEC-AM-2	Supplier will establish handling standards, including adding, transfer, removal and disposal of all assets based on asset classification. Process for maintaining hardware and software must be documented to include but not limited to asset control tag, physical location, asset owner, operating system, environment, etc.
Network Security	
SEC-NS-1	Supplier agrees to maintain network security that, at a minimum, includes network firewall/security groups provisioning, intrusion detection and/or prevention, and monthly vulnerability assessments.
SEC-NS-2	Supplier agrees to maintain network security that conforms to generally recognized industry standards and best practices (e.g. Center for Internet Security, PCI, NIST, ISO/IEC 27000-series, Cloud Security Alliance, Organization for the Advancement of Structured Information Standards, etc.) that Supplier then applies to its own network.
SEC-NS-3	No Supplier connections to the Customer network are permitted without first being subjected to a security risk assessment to assess any risks the Supplier's connection may pose to the integrity of the Customer network, equipment and information resources. This requirement extends to any third-party subcontractors Supplier may employ to support the Services.
SEC-NS-4	Supplier agrees to notify Customer when material architecture changes are made to the technology interface used to connect to the Customer network to allow a re-assessment.
SEC-NS-5	Supplier must ensure that controls are in place on all equipment, systems and networks connected to the Customer network to prevent and detect the introduction and proliferation of malicious code. The controls must be (i) continuously enabled when supported by the device; and (ii) updated on at a minimum daily to guard against new threats and support security patches. All electronic files, such as program and executable files, data files, e-mails, and e-mail attachments introduced into the internal network must be scanned for the presence of malicious code prior to entering the network.
SEC-NS-6	Supplier's personnel and subcontractors connected to the Customer must immediately disconnect systems from the Customer network that have detected or suspect an attack by malicious code and notify Customer immediately.
SEC-NS-7	Supplier must ensure that security events be logged (log files), monitored (appropriate individuals). and addressed (timely action documented and performed). Organizational responsibility for responding to events must be defined. Configuration checking tools must be utilized, or other logs must be utilized, that record critical system configuration changes. The log permission must restrict alteration by administrators. Retention schedule for various logs must be defined and adhered.
Application Security	
SEC-AS-1	Supplier agrees to provide, maintain, and support its software and subsequent updates, upgrades, and bug fixes such that the software is, and remains secure from those vulnerabilities as identified by industry experts and authorities (e.g. OWASP, CWE/SANS, etc.)
SEC-AS-2	Externally connected operational systems and application software must be subject to strict change control.
SEC-AS-3	Supplier's personnel and subcontractors must not intentionally write, generate, compile, copy, collect, propagate, execute or attempt to introduce any computer code designed to self-replicate, damage or otherwise hinder the performance of any Customer system or network.
SEC-AS-4	Supplier agrees to implement monthly network and application vulnerability scanning.
SEC-AS-5	Supplier agrees to remediate identified vulnerabilities classified by scanning vendor as Critical or High within 30 days of identification; Medium vulnerabilities within 90 days and Low vulnerabilities within 120 days of identification.
SEC-AS-6	Supplier agrees to an annual penetration testing by an external entity covering all systems and applications providing services to Customer.
Data Security	

SEC-DS-1	Supplier agrees to preserve the confidentiality, integrity and availability of Customer data with administrative, technical and physical measures that conform to generally recognized industry standards and best practices (e.g. Center for Internet Security, PCI, NIST, ISO/IEC 27000-series, Cloud Security Alliance, Organization for the Advancement of Structured Information Standards, etc.) that the Supplier(s) then applies to its own processing environment.
SEC-DS-2	Should Supplier handle cardholder data or sensitive authentication information, Supplier certifies that their Information Technology practices conform to and meet all then current Payment Card Industry Data Security Standards as defined by the Payment Card Industry Security Standards Council at https://www.pcisecuritystandards.org, and that it will provide to Customer, upon request, copies of Supplier's applicable Attestations of Compliance.
SEC-DS-3	Supplier must only use Supplier approved equipment and information resources when connecting to Customer systems or network.
SEC-DS-4	Supplier agrees that any and all data exchanged shall be used expressly and solely for the purposes enumerated in the current Agreement and/or Addendum. Data shall not be distributed, repurposed, or shared across other applications, environments, or business units of Supplier. Supplier further agrees that no Customer data of any kind shall be transmitted, exchanged, or otherwise passed to other Suppliers or interested parties except on a case-by-case basis as specifically agreed to in writing by Customer.
SEC-DS-5	Supplier agrees that all data, defined as confidential or personally identifiable information under current legislation, regulation or contractual obligations, stored on Supplier's mobile computing devices, laptops, backup media. or portable storage media, be encrypted and protected against unauthorized access.
SEC-DS-6	Supplier must ensure that all Cox Automotive (or its Affiliates') customer data must always be encrypted at rest when stored with the Supplier's systems.
SEC-DS7	Supplier agrees that upon termination of this Agreement, it shall permanently erase, destroy, and render unrecoverable all Customer data and certify in writing that these actions have been completed within 30 days of the termination of this Agreement or within 7 days of the request of an agent of Customer, whichever shall come first.
SEC- DS-8	Supplier agrees that all electronic transmission or exchange of system and application data with Customer and/or any other parties shall take place via secure means (e.g. using HTTPS, TLS, Secure FTP or equivalent)
SEC-DS-9	All transmission of all Customer data must be encrypted when outside the Supplier's network.
SEC-DS-10	Mobile computing must be performed over encrypted channels.
SEC-DS-11	All mobile devices (mobile phones, laptops, tablets) used to provided services to Customer must be encrypted. Mobile Device Management (MDM) solution must be implemented to enforce encryption, passcode and remote wipe for mobile devices.
SEC-DS-12	Data Loss Prevention (DLP) system, filtering products) must be in place to prevent Customer Confidential Information from being sent externally through both internal and external email without encryption. Preventive and detective controls must block malicious e-mails/ attachments. Policy must prohibit auto-forwarding of emails. Additionally, Cloud based systems providing services to Customer must implement DLP solution to prevent confidential Customer from leaving cloud-based systems.
Personnel and Organization	
SEC-PO-1	Supplier is solely responsible for ensuring the personal reliability and integrity of Supplier personnel and subcontractors who are granted access to Customer information resources. Supplier must be able to prove, if requested, that appropriate employee and subcontractor background checks were performed prior to granting access to information resources. Anyone having been convicted of a misdemeanor offense relating to computer security or any felony will not be granted access to Customer information resources. Customer reserves the right to refuse or revoke access of any Supplier personnel or subcontractor convicted of any misdemeanor offense related to computer security or any felony.
SEC-PO-2	Supplier personnel and subcontractors with access to or in possession of non-public information must adhere to all confidentiality requirements set forth in the Agreement or other applicable document with Customer.
SEC-PO-3	Supplier must ensure that Supplier personnel and subcontractors with access to the network, systems and information (electronic or hardcopy) are provided sufficient training and supporting reference material to enable them to properly protect the confidentiality, integrity and availability of information resources. At a minimum Supplier personnel and subcontractors will receive annual security awareness training.
SEC-PO-5	Supplier shall ensure that an appropriate authentication system will be put in place to authenticate valid users.
SEC-PO-6	All Supplier access to Customer's systems or network resources must be initiated from within the United States unless prior authorization is granted in writing, by an authorized Customer representative.

SEC-PO-7	Supplier is responsible for ensuring all personnel and subcontractors are informed of and apply secure best practices when using Customer's network, systems, and information resources.
Right to Audit	
SEC-RR-1	Customer reserves the right to perform an on-site audit of the Supplier's support environment and Information Security practices, using internal or prior approved independent third-party auditors. Notification of such audit must be provided to Supplier at least 10 business days prior to the requested audit start date.
SEC-RR-2	Customer reserves the right to request a security vulnerability test of Supplier's applications and systems and any portion of Supplier's IT infrastructure used to support the services being provided to Customer.
Access Control	
SEC-AC-1	Supplier must ensure that every user has a single unique user ID and a personal secret password for access to the Supplier's network, equipment and information. Remote access must require multi-factor authentication.
SEC-AC-2	When supported on Supplier's systems, passwords that allow access to Customer information must comply with the following standards: (i) passwords must be changed at least every ninety (90) days; (ii) systems must not allow users to change their password more than once within a seventy-two (72) hour period without the involvement of a security administrator or help desk function; and (iii) account lockout must occur after a maximum of five (5) failed password entry attempts. Re-enabling of locked accounts must require interaction with a security administrator or help desk function.
SEC-AC-3	Passwords used by Supplier personnel and subcontractors to access Supplier's networks and information resources must comply with the following standards: (i) must not employ structure or characteristic that results in a password that is predictable or easily guessed including, without limitation, words in a dictionary, derivatives of user IDs, common character sequences, personal details, or any part of speech; and where technically feasible, (ii) be at least eight characters in length, and (iii) include at least three (3) of the following character sets, in accordance with password policy settings: (1) an English uppercase character (A – Z); (2) an English lowercase character (a – z); (3) a westernized Arabic numeral; and (4) a non-alphanumeric special character.
SEC-AC-4	Access rights must be controlled based on the "least access" principle, which grants the minimum access permission required to meet the business need. Supplier will ensure that privileged access (e.g. sysadmin, root, superuser, etc.) to Supplier network devices and systems that connect to Customer information resources are restricted to those personnel and subcontractors with a valid business need.
SEC-AC-5	Supplier personnel and subcontractors must maintain exclusive control of their Cox user ID and password to prevent disclosure to unauthorized personnel. Passwords and user IDs must not be shared with other users or stored in clear text format in any location where unauthorized persons might discover such IDs or passwords.
SEC-SC-6	Supplier personnel and subcontractors must immediately change any user IDs or passwords that provide access to internal network and systems if the IDs or passwords are suspected or known to have been compromised by disclosure to unauthorized persons. Supplier personnel and subcontractors must not store fixed passwords used to access networks and systems in communications programs, Internet browsers or related data communications software. Passwords must also not be stored in readable form in batch files, automatic login scripts, software macros or terminal function keys.
SEC-PO-4	Supplier must establish and have a process in place to immediately notify Customer of all Supplier personnel and subcontractors who leave the Supplier's company or who no longer have a valid business need to access Customer's information resources, to ensure their access is removed in a timely manner.
SEC-SC-7	Supplier personnel and subcontractors must not attempt to access any Customer host or network without specific authorization. All Supplier connections to the internal network, including, without limitation, any connections remote to Supplier's primary location, must use only communications connections with prior approval. Supplier personnel and subcontractors requiring access to the internal network must be approved, in advance, prior to accessing the network or any Customer owned equipment or information resources accessible from the internal network. Only prior approved software and equipment may be used to connect to the internal network.
Security Breach Notification and Incident Management	
SEC-SB-1	Supplier must have a process to detect and respond to a suspected or confirmed breach of security of any Customer information resources. Supplier will notify Customer at infosec@coxautoinc.com within 48 (forty-eight) hours of the determination of the suspected or confirmed breach and will secure its systems as soon as is reasonably possible.
SEC-SB-2	Supplier shall keep Customer informed of all progress and actions taken in connection with Supplier's investigation of all incidents involving the suspected compromise of Customer information resources. Supplier shall provide any information deemed necessary to assist with the investigation.

SEC-SB-3	Unless such disclosure is mandated by applicable law or regulation, Customer, in its sole discretion, shall determine whether to provide notification to customers, employees, agents or government authorities concerning a breach or potential breach of privacy or any other type or form of security incident.
SEC-SB4	Supplier must have a documented information security incident management process regarding incidents relating to the network, equipment and information. The information security incident management lifecycle process must include: (i) identifying and reporting information security incidents; (ii) responding to security incidents; (iii) recovering from information security incidents; and (iv) following up with information relating to security incidents.