Product Cybersecurity Policy

I. Purpose

General Motors places its customers at the center of everything it does. The protection of vehicle electronics systems and data from unauthorized outside electronic access or control is important for the safety and security of GM's customers. It is important that GM products are safe for our customers and contain reasonable security. This includes, but is not limited to, protecting vehicle electrical systems, theft deterrent systems, connected telematics and infotainment systems, advanced driver assistance systems, and services that interact between IT infrastructure and the vehicle. All persons involved in the development of GM vehicles, vehicle systems or connected vehicle services must understand the importance of cybersecurity in protecting GM customers, GM, and their data. To aid in achieving these protections, Product Cybersecurity focuses on the following key areas:

1) Security of vehicle electronic control systems from unauthorized outside access, including but not limited to protecting the safety of the customer; and
2) Security of the customer's data available by or through the vehicle, or in connection with connected vehicle services, including Personal Information data.

To enable these key focus areas, Product Cybersecurity maintains appropriate security standards, practices, guidelines and controls aimed at defending the vehicle and vehicle services ecosystem against unauthorized electronic access, detecting possible malicious activity in the related networks, and responding to suspected cybersecurity incidents in a timely, coordinated and effective manner.

This Product Cybersecurity Policy describes high level direction for product cybersecurity management and oversight. General Motors and its employees engaged in work that directly or indirectly affect any vehicle products or vehicle connected services offered or available to customers or end users must be able to demonstrate compliance with this Policy.

II. Applicability

This Policy applies to the following:

- All GM Operating Units for all vehicles and connected vehicle services developed by GM or provided to end users under a GM-owned brand, especially those employees that develop and release products and services, and those who establish contracts with and manage third parties that, in whole or in part, develop and release products and services.
- Any joint venture or subsidiary in which GM has management control and owns directly or indirectly more than fifty percent (50%) of the equity.
- This Policy is not retroactive.

III. Compliance

Compliance with this Policy is subject to oversight by the Product Cybersecurity organization, and as conditions warrant, audit by GM Audit Services and information security auditors.

IV. Definitions

GM Operating Units – All of GM and its subsidiaries in which GM owns over 50% of the equity or has day to day control of the business operations. This includes but is not limited to operations where GM designs, builds and/or sells its vehicles, service parts and vehicle connected services, such as assembly, stamping, powertrain and components operations, distribution centers, warehouses, training centers, technical and engineering centers, connected services operations centers, proving grounds, as well as corporate and marketing office buildings. GM Operating Unit does not include: a subsidiary (including a joint venture) in which GM owns directly or indirectly fifty percent (50%) or less of the equity or which GM otherwise does not have day-to-day control, third party suppliers, and dealerships.

Personal Information – This term has the meaning set forth in the Global Privacy Policy, PRIV-01.

Vehicle Technical Specification – Document or documents that define technical requirements for the vehicle development process and the technical definition of the vehicle's functional characteristics and requirements.

V. Policy

The following identifies security requirements for General Motors and all applicable entities:

1. Security by design shall be considered throughout all phases of applicable product and services development in accordance with security development lifecycle (SDLC) processes and requirements designated by GM Product Cybersecurity. All vehicle products and connected vehicle services that are available for customer or non-GM use must be developed using an SDLC process. This Policy recognizes that there is no single SDLC process and that multiple approaches to developing software, hardware, systems and services can each qualify as an SDLC process. Each SDLC process will have common security related practices, including: secure design, threat modeling, secure implementation/coding, design reviews, development reviews, scanning, verification and testing, approvals, vulnerability maintenance and remediation, and documentation of these practices. For each development process for vehicle software, products or connected services, the development and implementation owners must agree with Product Cybersecurity on the SDLC process to be integrated into the development process.

2. Vehicles, regardless of country of origin or manufacture, shall meet Vehicle Technical Specification requirements for cybersecurity.

3. Connected vehicle services used to exchange data between the vehicle and connected vehicle ecosystem (e.g., IT, cloud services, brought-in devices, V2X) shall meet requirements applicable to vehicle services as designated by Product Cybersecurity and applicable Information Security Requirements to ensure confidentiality, integrity, and availability of the services.

4. All third party contracts for development of vehicles, vehicle components or systems, or vehicle connected services should contain provisions supporting the goals of this Policy.

5. Deviations from this Policy will be considered under GM Product Cybersecurity risk assessment criteria and must be approved by the responsible Director in the GM Product Cybersecurity organization, with appropriate documentation following applicable corporate deviation processes.

VI. Policy Structure

This Policy is part of the overall management of Product Cybersecurity, which includes specifications, practices, and procedures relating to the development and implementation of products and services, including cybersecurity practices that GM has been and continues to implement.

This Policy supports GM's Code of Conduct, Winning With Integrity. You should report suspected violations of this Policy in accordance with GM's Code of Conduct and Speak Up! GM's Non-Retaliation Policy. GM does not tolerate retaliation against anyone who raises a concern in good faith.

This Policy is supported by GM's Information Security Policy and GM's Global Privacy Policy.

Executive in Charge:
Chief Product Cybersecurity Officer