GENERAL MOTORS

Global Information Security Policy

I. Purpose

General Motors Information (GM Information) is one of our most important assets and must be protected. GM Information exists in many forms, including but not limited to: text, image, and sound and can be found in numerous locations and storage devices. GM Information is owned by GM, wherever it exists, (e.g., personally owned Computing Equipment, Third Party-owned Computing Equipment, Mobile Devices).

All users of GM Information must understand its value and their responsibility to protect it. This Information Security Policy describes the high-level direction for information security that must be adhered to within the GM environment. It is based on the three fundamental security concepts:

- Confidentiality
- Integrity
- Availability

GM and the users of GM Information must be able to demonstrate that due diligence has been exercised in protecting GM Information. By performing due diligence, GM can successfully protect its rights to GM Information by, among other actions, taking appropriate legal action including referring the matter to government authorities for civil or criminal prosecution. Illegal, unauthorized, or unethical disclosure, modification, misuse, or disposal of GM Information is prohibited.

II. Executive in Charge, Policy Contact, Policy Interpretation

The Information Security Policy is the responsibility of the GM Senior Vice President and Global Chief Information Officer (Global CIO). The GM Senior Vice President and Global CIO has the authority to approve changes to the Policy. The GM Senior Vice President and Global CIO has delegated authority to interpret this policy to the GM Chief Information Security Officer (CISO). The Policy Contact for this policy is the GM CISO.

III. Applicability

This policy applies to the following:

- All Global Functions, Business Units, and Corporate Staffs, as well as
- Any subsidiary in which GM has management control and owns directly or indirectly more than fifty percent (50%) of the equity unless the subsidiary has been granted an exemption by the GM CISO

- All third party contract workers, suppliers, alliance partners, and joint venture partners who have been given written authority to access the GM computing environment

All Third Parties who collect, handle, manage, access, or store GM Information, external to the GM computing environment must comply with the Third Party Information Security Requirements.

IV. Superseded Document

This policy supersedes Information Security Policy, published September 30, 2014.

V. Compliance

Compliance with this policy is subject to audit by GM Audit Services, GM Information Security or Third Party Auditors.

GM has the right to review, audit, or monitor, in accordance with applicable laws:

- All GM Information, data, and computing and communication resources utilized to support GM business;
- Business process activities, information, data, and computing and communication resources of non-General Motors providers that support GM business;
- Personal information, data, image, video or voice stored or recorded within a GM computing or communication resource, (e.g., electronic-mail, laptops/notebooks, voice mail, and removable media).

General Motors also has the right to periodically request a self-assessment or other confirmation of compliance with these Policies by non-General Motors providers that support General Motors business and other custodians of GM Information.

Any requests for deviations to this Policy must follow the Information Security Deviation Request Process.

VI. Definitions

Availability - Ensures that information is accessible when and where it is needed.

Computing equipment - Any automated device or system used to manage or store information.

Confidentiality - Ensures that Information is not disclosed to anyone who is not authorized.

Contract Worker - A person who performs services for GM pursuant to an agreement between GM and the person's employer. A Contract Worker is not a GM employee and remains subject to the control and employment terms of the Contract Worker's own employer.

GM Computing and Communication Network - The hardware and software components that support the movement of GM Information from one device to another.

GM Employees - Workers and staff directly hired and paid by GM, entitled to GM benefits and subject to GM terms of employment, Policies and Controls.

GM Information - All information, physical and electronic or otherwise, relating to the business of GM and created or acquired using its resources. All GM Information is the sole property of GM. GM Information exists in many forms, including but not limited to product plans, vehicle designs, product prototypes, strategy documents, business records, nonbusiness records, pricing information, financial or technical data, and text, sound or image files.

Integrity - Ensures that information is correct or accurate to the degree anticipated by those who use it. It also ensures that information has not been changed and has not been exposed to unauthorized modification.

Malware - Malicious code which performs a series of harmful actions within a computer system or on infrastructure components (e.g., Viruses, Trojan Horses, and Worms).

Mobile Device - Small, portable, electronic devices that connect to GM proprietary systems or information (e.g., smart phones, tablet PC, PDAs).

Third Party - A person, company, business, organization, or group that 1) conducts business with, provides goods or services to, directly or indirectly, or is a customer of General Motors or 2) is a competitor of General Motors. Third Party includes but is not limited to dealers, Alliance Partners, consultants, professional service providers and business partners. These entities may create, collect, manage, process, access, store or transmit GM Information or represent GM in the course of business.

Users - GM employees, Contract Workers and authorized Third Parties accessing GM systems or IT Resources.

VII. Policy

1. Key Requirements

The following identifies information security requirements for GM and custodians of GM Information:

a. Information, in any form, relating to the business of GM and created or acquired using its resources, whether such information is owned or licensed by GM, must be protected from unauthorized disclosure or modification, Malware, misuse, and improper disposal, whether intentional or unintentional.

b. GM Information, when created or acquired, must be assessed and classified according to its value and sensitivity to disclosure and must be managed accordingly.
c. The importance of GM Information, as well as its computing and communication environment, must be assessed and appropriate plans must be put in place to mitigate potential loss of GM Information.
d. Any Third Party information possessed by GM must be protected in accordance with the terms of any agreements with the Third Party, or, in the absence of such an agreement, with any other controls or mechanisms that may be established by a GM business unit.
e. GM, its employees, Users and custodians of GM Information must comply with all local laws within each GM business unit location, regulations and all contractual agreements specifying information security controls, (e.g., copyright, patents, cross-border transfer of information and technology, import and export regulations, Confidentiality and non-compete requirements).
f. Suspicion or occurrence of any fraudulent activity, unauthorized disclosure, modification, misuse, or disposal of GM Information, including intrusions or incidents of impaired or denied Availability to the GM computing and communications environment must be reported promptly to management or through GM's established reporting processes (e.g. Awareline).
g. Management must ensure their employees and contractors are aware of established security policies and must take appropriate action upon violation of established security policy.
h. The Information Security organization must provide appropriate awareness training to inform Users of their responsibilities to protect GM Information.

2. Roles and Responsibilities

a. GM Information Security Policy and Standards
   - The GM Senior Vice President and Global CIO is responsible for the approval of the GM Information Security Policies and Standards.
   - The GM Chief Information Security Officer (CISO), under the direction of the GM Senior Vice President and Global CIO supports the development of the Information Security Policies and Standards.
   - The GM Information Security Policies and Standards shall be reviewed and revised by the GM CISO on a periodic basis.
   - The GM CISO ensures the GM Information Security Policies and Standards are published, and communicated to all affected units.

b. All GM employees are responsible for the implementation of Information Security Policies

Executive in Charge:
Chief Information Officer