

# General Motors IT Standards

## Overview

GM has adopted a set of information technology infrastructure standards for the Dealer internal network environment to ensure a seamless and reliable conduit for the GM Corporation to Dealer communication channel. With the continuous growth of technology and hence the continuing evolution of these GM Dealer standards, it is important to maximize your I.T. investment. To help dealers get the most out of their IT dollar hardware specs are organized by minimum (what is needed to effectively communicate with General Motors) and Recommended (what should be procured at this time to maximize the lifecycle of the investment). Dealer IT standards are posted to [www.GMDIT.com/standards](http://www.GMDIT.com/standards). They are also available in Global Connect.

## How do these dealer IT standards benefit me/ my dealership?

The proper network infrastructure will make it easier and more efficient to do business. Slow network/ Global Connect performance (due to things such as the wrong equipment, spy ware or viruses) can cost money due to downtime, maintenance, or even loss of employee productivity. General Motor's applications are designed to work efficiently with business grade hardware and services. Make sure you have the correct Network infrastructure in place to effectively utilize Work Bench applications to their fullest intended purpose.

## How do these standards relate to data security?

*Protecting your customer's data is your responsibility.* Neglecting these responsibilities can lead to legal action, penalties, and fines from the FTC or Credit Card Industry. Security specifications were clarified in the latest version of the dealer IT Standards to give a more detailed description of what is needed to properly protect customer information. These include:

### Minimum:

- ✓ Designate an employee (Dealer direct possibly your PSC) to be in charge of security policies, procedures, and FTC required paperwork.
- ✓ Regularly perform a Risk Assessment to identify foreseeable risks.
- ✓ Implement "Reasonable measures" to control risks. Including:
  - Up-to-date security device that continually monitors threats through intrusion detection and prevention system.

### Recommended:

- ✓ Fully managed security device that continually monitors threats through intrusion detection and prevention system (IDS and IPS) and other mechanisms.
- ✓ Web filtering and monitor websites visited to block inappropriate or entertainment orientated websites that are the most dangerous source for inadvertently downloading malicious programs.

For more information: Go to [www.GMDIT.com/security](http://www.GMDIT.com/security). Or contact a GMDIT network specialist at 866-526-8333.

