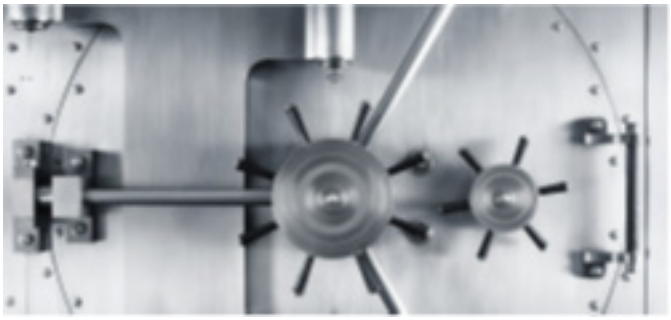
DELL Technologies



Dell SafeSupply Chain

Commercial

Optimize Endpoint Security

Security-sensitive organizations are becoming increasingly aware of the potential threats to Information and Communication Technology (ICT) supply chains. Threats continue to evolve as nefarious actors try to take advantage of any weak link in the supply chain that will allow them to gain access to protected information or to disrupt a corporations day to day activities. Threats include malware, coding vulnerabilities, and counterfeit electronic components that are inserted into products within the supply chain - any time between the initial design and development of the product through actual delivery to customers. Recognizing this potential risk to the business, Dell continues the development of stronger ICT supply chain security solutions.

Dell Technologies is committed to being the preferred supplier of end-to-end, cutting-edge technology solutions to customers to provide added security straight out of the box. Dell leverages a robust Supply Chain Risk Management (SCRM) Program to ensure foundational controls for all product supply chains meet or exceed customer expectations and industry standards. The program focuses on giving customers the confidence that the products acquired from Dell Technologies are exactly what they expect them to be, nothing more and nothing less, and that they will operate as intended. This is accomplished through an evolving strategy that relies on multiple layers of supply chain security and integrity controls throughout the entire supply chain lifecycle.

Delivering Trustworthy Products Straight Out of the Box

Dell Technologies Supply Chain Standard Practices

Dell's intent is to fulfill customer requirements with authentic, Dell-branded systems and accessories. As the OEM, Dell can ensure that the customer receives products that come through Dell-authorized channels. Preventative and detective control measures that protect physical assets, inventory, information, intellectual property and people include the following:

- Customer Information Security (CIS) controls and requires annual employee compliance training.
- All employees submit to appropriate background checks in accordance with local laws and regulations and all employees working in the Dell U.S. are U.S. citizens.
- Certified C-TPAT partner working with U.S. Customs and Border Protection (CBP) and other principle stakeholders of the international supply chain community to identify potential security gaps, and implement specific security measures and best practices to advance protection of the global supply chain. All Dell Client Products (desktops, laptops, and All-in-Ones) and PowerEdge Servers have been certified at Tier 3 while products other than Dell Clients and PowerEdge Servers have been certified at Tier 2.
- Accredited member of Transported Asset Protection Association (TAPA) and follows TAPA FSR (Freight Security Requirements) standards for the purpose of addressing cargo security threats that are common to the high tech industry. Dell logistics and transportation providers are required to be TAPA "A" compliant.

- Product design incorporates Secure Development lifecycle (SDL) based on industry standards (ISO/IEC 27034) and best practices (SAFECode).
- Product designs include BIOS protections in accordance with NIST 800-147 guidelines. All Dell BIOS development and coding is performed or managed by Dell employees.
- Manufacturing conducts SHA-256 hash verification on the BIOS for all laptops, desktops and servers prior to shipping as part of the integrated Anti-Tamper program intended to protect critical technology information.
- Laptop, desktop, and server manufacturing requires key component suppliers to affix a unique Piece Part Identification Number (PPID) label to specific parts to identify and track individual components. PPID numbers contain not only the manufacturing date of a component, but also information regarding the supplier, the country of origin, and the Dell part number. Key components that are smaller in size, like processors and memory, are identified using an electronic identifier that is captured during manufacturing. Dell EMC storage products capture the serial numbers of key components along with the associated date and lot codes at all suppliers. This information is stored within their shop floor control systems. Each of these suppliers can be confirmed against the Dell Storage Approved Manufacturer List (AML).
- The supply chain maintains compliance with DFARS 252.246-7007, Contractor Counterfeit Electronic Part Detection and Avoidance System, and DFARS 252.246-7008, Sources of Electronic Parts.
- Compliance with the ISO 9001 quality management system to include product design, development, procurement, manufacture, fulfillment, delivery, sales operations, customer service, take-back & recycling, refurbishment and supporting function of computers, storage and server products, technology products, services and solutions.

What is Dell's SafeSupply Chain Program?

Many security-sensitive customers already require suppliers to comply with industry-standard protections, regulations or relevant guidelines that have been published by organizations such as the National Institute of Science and Technology (NIST). However, quite a few have determined that they need to go above and beyond common ICT practices to mitigate further risk. Implementing additional requirements will result in a higher level of confidence and trust in the ICT products they acquire.

As a result, Dell has launched the SafeSupply Chain program that focuses on two discrete layers of protection – all while maintaining competitive pricing and industry-leading quality and support.

Tamper Evidence	Device Sanitization
• Dell **tamper-evident seals** added to seal the system before shipping to final destination • Dell **tamper-evident tape** added to seal the system box • Dell **tamper-evident pallet seals** added before shipping to final destination	• **NIST 800-88 secure hard drive wipe*** mitigates the risk of a compromised hard drive prior to imaging – **NIST 800-88 Clear** wipe & sanitization for SSD drives – **NIST 800-88 Purge** wipe & sanitization for HDD drives • **Hard drive re-imaging** according to customer contract specifications

*Dell's approach to the handling of data storage devices is to either:
1. Sanitize the device (in alignment with the US Department of Commerce NIST SP 800-88 Rv. 1"Purge" or "Clear" methods) in preparation for reuse;
2. In the event that Dell determines that the device cannot be secured through sanitization, Dell will destroy the device using physical shredding or such other appropriate physical destruction method (in preparation for recycling, and in accordance with the US Department of Commerce NIST SP 800-88 Rv. 1 "Destroy" method).

**Dell performs regular audits of its own facilities and operations, as well as its partners and suppliers who are authorized to perform data security processes regarding physical security and sanitization.

For more information, please contact your Dell Technologies Services Representative.