HP'S PRODUCT SUPPLY CHAIN SECURITY

HP takes Product Supply Chain Cybersecurity very seriously and understands that it is the entry point for mitigating the risk of counterfeits, malware, or tampering of our products. It begins with extensive vetting of our supply base all the way from the component level to our logistics partners.

For our suppliers to meet the expectations our customers have placed on us, we developed a Product Cybersecurity Standard that lists requirements designed to protect the integrity of our products.

4AA7-4216ENW, January 2020

Product Supply Chain Cybersecurity

Setting the Standard for Suppliers, Manufacturing Partners, and Logistics Partners

- Product Design & SDLC
- Electronic part sourcing and procurement
- Software & Firmware installation
- Manufacturing controls
- Sub-Supplier Management
- Physical Security
- Transportation & Storage

Some examples of key requirements:

- Outsourced product design: for our ODM Suppliers we ensure they follow Secure Development Life Cycle best practices and conduct penetration testing against all known exploitation tactics
- Electronic part sourcing: ensures all electronic components meet US DoD DFARS 252.246-7008 - Sources of Electronic Parts for all products worldwide
- SW/FW installation: strict protocols and procedures for the loading of firmware, software and customer images in a controlled secure environment
- Manufacturing controls: running anti-malware scans on all systems used to support or produce product, using current operating systems, establishing a secure environment for IT systems
- Sub-supplier management: flow down the requirements to all levels of our Supply Chain
- Notifications: clear escalation path for all levels of breaches to the requirements
- Transportation, storage & physical security: technology to prevent loss, overt and covert tracking, real time monitoring to review anomalies such as route deviation or unscheduled stops, alarm systems, security guards, restricted sections, video surveillance cameras, and perimeter fencing

4AA7-4216ENW, January 2020

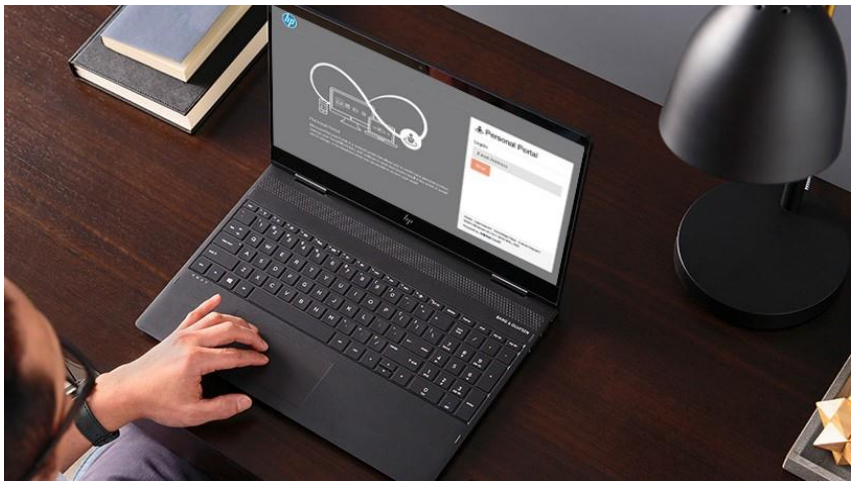
Software Imaging Security

HP recognizes the fundamental importance of privacy, security, and data protection in the deployment and delivery of personal system assets to our customers. HP secures the loading and licensing of software images/firmware on personal systems shipped, which is in keeping with HP's strategic objective of producing best in class secure products. HP PSO (Personal System Operations) has obtained ISO 27001:2013 security certifications of the Image Load process and Dynamic Configuration Service.

The software image comprises the OS, requested 3rd party applications, and diagnostic tools required to support the operation of the system requested by customers. The Image Load process covers the end-to-end process of placing a verified and validated image onto systems. Dynamic Configuration Service allows customers to extend the imaging environment into HP's factories or staging centers through a secure VPN connection – so customers will be able to control the configuration activities for new products prior to shipment. With this connection, customers can directly manage and configure images, applications, domain join, HDD encryption, BIOS settings, and unit personalization.

HP Product Security and Privacy

As cyberattacks become increasingly prevalent and sophisticated, security breaches are a growing concern for our customers. In response, we are continually evolving HP products, solutions, and services to offer industry-leading resiliency capabilities that anticipate an ever-evolving attack and threat landscape.



We follow security and privacy by design principles for all our products, from design through customer use, refurbishment, and recycling. We build protection, detection, and recovery into the entire device, not just the software, which provides customers with separate, auditable mechanisms for managing security risks. To protect against the malware of the future, PCs and printers must have hardware-level security that seamlessly integrates with the customers' broader IT network security infrastructure. This is the foundation of HP's strategy.

4AA7-4216ENW, January 2020

Our Security Management Review Committee, composed of business leaders from across the company, oversees and aligns our portfolio-wide approach to security and provides necessary resources to support HP's continued leadership. An external Security Advisory Board was launched in 2017 to provide insights that HP uses to reinforce its own security work. All three founding members have unique first-hand expertise in the world of hacking and the latest developments in security technology and strategies.

We employ cybersecurity specialists and conduct cybersecurity architecture reviews, penetration testing, code reviews, and automated code scanning using industry-leading tools. When issues arise, we take appropriate actions to remediate reported security vulnerabilities, as committed in HP's Coordinated Vulnerability Disclosure policy.

4AA7-4216ENW, January 2020