



## PCI COMPLIANT HOSTING

**GO FROM ZERO TO SIXTY WITH  
PCI COMPLIANT INFRASTRUCTURE**

# PCI COMPLIANT HOSTING

## GO FROM ZERO TO SIXTY WITH PCI COMPLIANT INFRASTRUCTURE

### 🌱 LIGHTCREST PCI COMPLIANT HOSTING

Lightcrest provides secure web hosting to customers around the world. If your company stores, accepts, or processes credit cards, it is in your best interest to maintain PCI DSS compliance, a value-add that you can pass on to your customers and an edge you can boast to win new business.

Whether you want a cluster of machines or VPS systems segregated virtually, Lightcrest will ensure your database and applications layers are segmented, firewalled, and reinforced with authentication and retention policies to keep you compliant and secure without compromising performance and reliability. Additionally, Lightcrest can provide add-ons in the form of automated audit trail collectors, scheduled port scans and file system checks, and custom kernel modules to immediately alert you of malicious file-system operations.

### 🌱 DO YOU NEED PCI DSS?

If you process, store, or transact cardholder data, you should be PCI DSS compliant. While it is not yet required by law, it is critical that you impress upon your customers, partners, and processors that you are keeping sensitive cardholder data secure at every layer of your technology infrastructure.

Lightcrest provides PCI compliance to customers who demand immediate turn-around on newly deployed financial applications, whether they be payment gateways, e-commerce applications, online banking interfaces, or transaction databases. PCI DSS can be expensive to implement in house - Lightcrest provides the compliant infrastructure customers need at a fraction of the in-house cost.

### 🌱 WHAT IS SENSITIVE ACCOUNT DATA?

PCI DSS applies wherever account data is transmitted, processed, or stored. According to PCI DSS v2.0 standards, sensitive data includes Cardholder Data and Sensitive Authentication Data.

#### Cardholder Data Includes:

- Primary Account Number
- Cardholder Name
- Expiration Date
- Service Code

#### Sensitive Authentication Data Includes:

- Full Magnetic Stripe Data (or on-chip equivalent)
- CAV2/CVC2/CW2/CID
- PINs/PIN Blocks

### 🌱 FROM THE PCI SECURITY STANDARDS COUNCIL

*"The primary account number is the defining factor in the applicability of PCI DSS requirements. PCI DSS requirements are applicable if a primary account number (PAN) is stored, processed, or transmitted. If PAN is not stored, processed or transmitted, PCI DSS requirements do not apply."*

When considering an MSP in conjunction with PCI requirements, it's critical that you partner with a provider that is not only an expert in PCI but also in disaster recovery, high-availability, and fully managed hosting operations.

If you need PCI DSS compliance, or are considering hardening your systems in preparation for an audit, **contact us now.**



## EXAMPLE PCI DSS REQUIRED PRECAUTIONS

- Hardened & synchronized firewalls
- Penetration testing
- Vulnerability scanning
- Hardened DMZ
- Stateful packet inspection
- Anti-Virus and software firewalls on desktops and mobile devices
- System Configuration Standardization (e.g. CIS, ISO, SANS, NIST)
- One core service function per system
- Hardened and stripped servers
- Removal of unnecessary runtimes
- End-to-End encryption (SSH, VPN, SSL/TLS)
- Deletion of stored data after maximum retention period
- Audit trails and system log management



  
**Lightcrest**

11835 WEST OLYMPIC BLVD. SUITE 415E, LOS ANGELES, CA 90064 | 888.320.8495 | [www.lightcrest.com](http://www.lightcrest.com)