PCI DSS

Summary

Regulation: Payment Card Industry Data Security Standard

Abbreviation: PCI DSS

Governs these parties: any business that accepts card payments, including seasonal or small businesses

Enforced by: Visa, Mastercard, AmEx, JCB, and Discover

Details

PCI (or payment card industry) compliance is the set of policies and procedures developed to protect credit, debit, and cash card transactions and prevent the misuse of cardholders' personal information.

Any business that transmits, stores, handles or accepts credit card data need to be defended against ransomware, exploits, and adversaries. In order to comply with PCI DSS, you should restrict access to stored cardholder data, and secure, track and monitor access to network resources with encrypted transmissions.

The rest of this document is designed to help our community understand PCI DSS better by outlining the following information.

How it Relates to Cybersecurity

PCI compliance refers to a set of 12 security standards that businesses must use when accepting, transmitting, processing, and storing credit card data:

1. Install and maintain a firewall, including testing network connections, and restricting connections to untrusted networks.
2. Change vendor-supplied default passwords and security settings, including enabling only necessary services, removing functionality where warranted, and encrypting access.
3. Protect stored cardholder data, including having policies for disposing of data, limiting what is stored, and avoiding storing certain types of data.
4. Encrypt cardholder data when transmitting it across open, public networks.