Pete's Pizza Security Report

Prepared by: Dakota Bridges, Head of IT

Date: 11/14/2024

Adhering to PCI DSS requirements is imperative to Pete's Pizza's operations and furthermore our reputation as trusted local business. Diligent safety protocols will ensure the confidentiality of our customers cardholder data and personal information. These practices will also save money and resources in the future by preventing data breaches and cyber attacks. I have decided that we will focus on four areas of PCI DSS requirements: "restricting access to system components and cardholder data to need to know personnel", "protect all systems and networks from malicious software", "restricting physical access to cardholder data", and "protecting cardholder data with strong cryptography during transmission".

By restricting access of systems and cardholder data to only those whose job responsibilities require such access, we are protecting not only our customers but our other employees, such as bussing staff, from liability in the future. Being a small business, it is not uncommon to experience rates of high turnover. Currently this increases the number of potential employees with access they should not have. We will achieve this requirement by implementing role-based access controls and access groups via Microsoft Azure Active Directory and Intune. Since we're under 50,000 active users, this is something we can likely implement for free or of little cost to our company. Via Active Directory we can also implement semi annual automated audits of file shares, web servers, computers, and any device on our domain with no additional cost on resources.

Going hand in hand with this implementation will be to protect all systems and networks from malicious software. Smaller businesses often incorrectly assume they are not a priority for cyber crime. In reality it is because of our limited resources and defenses that we are far more likely to experience a serious attack. We will be combatting this by implementing quarterly patching and maintenance schedules for our systems in house. This includes verifying our antivirus software stays up to date and configured appropriately. We will coordinate at a later date to discuss change management procedures such as making sure we have backups of our systems, understanding the criticality of the environments being maintained, and preparing the schedule to make sure it does not interfere with our day-to-day operations. Furthermore, our point of sale terminals will be restricted from outside network access, ensuring that their only use-case is for their designated purpose. This can be done in coordination with the vendor as well to ensure they are configured correctly.

Going forward I recommend that we must restrict physical access to cardholder data. Our POS terminals will be tethered physically to our counter and other physical data relating to cardholder information will be stored in a safe away from the main dining area and common employee areas. These measures will prevent opportunistic criminals or bad actors from acquiring our customer's data.

Lastly, protecting our cardholder information with strong cryptography during transmission is essential to ensure that the data remains confidential. Our POS terminals will

need to use TLS 1.2 or higher as per compliance with PCI DSS. We will employ secure protocols such as HTTPS on our web servers as well. It is paramount to keep protocols up-to-date because outdated standards are more vulnerable to attacks.

These outlined strategies, protocols, and procedures will guarantee that not only Pete's Pizza adheres to the global standard, but also safeguards our customer's data. With the efforts of the IT Department and your approval, I believe that not only will our security be bolstered but this will solidify our reputation as a trusted local business. As with all areas of cyber technology, attacks and threats from criminals are more prevalent than ever. By being proactive with our security this will save our company time and money in the future.