PCI Compliance: Your Role in Protecting Customer Data

As an employee, you play a vital role in safeguarding our customers' sensitive information. By following these simple guidelines, you can help maintain PCI compliance and protect our business from potential security breaches.

Handling Cardholder Data

- **Limit Access:** Only handle cardholder data when necessary for your job duties.
- **Shred Sensitive Documents:** Properly dispose of any documents containing cardholder data by shredding them.
- **Avoid Storing Sensitive Information:** Do not store full card numbers, expiration dates, and CVV codes. If cardholder data must be stored, ensure it is in a secure location.
- **Encrypt Sensitive Data:** Use encryption tools to protect cardholder data when it's being transmitted or stored electronically.

Protecting Systems and Networks

- **Strong Passwords:** Create strong, unique passwords for all your company accounts. PCI 4.0 requires 12 characters in length and a combination of upper- and lower-case letters and special characters. Passwords should be changed every 90 days and multi-factor authentication (MFA) is encouraged when possible.
- **Be Wary of Phishing Attacks:** Avoid clicking on suspicious links or downloading attachments from unknown senders.
- **Report Suspicious Activity:** If you notice any unusual activity, such as unauthorized access or data breaches, report it immediately to your supervisor or the IT department.
- **Device Maintenance:** Check devices for tampering on a regular basis and maintain a list of active devices.

Additional Tips

- **Be Mindful of Social Engineering**: Be cautious of unsolicited requests for information, even if they seem legitimate.
- **Secure Your Workstation**: Lock your computer when you step away, even for a short period.
- **Review Policies**: Review company security policies on a regular basis.

By following these best practices, you contribute to a safer and more secure work environment for our customers and our business.