Best Practices for Credit Card Processing

- NEVER e-mail credit card information.
- Only employees who have a legitimate business “need-to-know” should have access to cardholder information.
- Sanitize credit card numbers on any document where the complete number is visible.
- Blackout credit card number (first 12 digits) and then photocopy.
- Shred the original, retain the copy.
- Cut out/off and shred card information. Do not use wireless networks for the processing of Credit Cards.

- Protect computer networks with hardware firewall and intrusion detection / protection.
- Separate and encrypt credit card processing traffic from regular traffic.
- Do not store credit card information online, if possible.
- If it is; Separate with a hardware firewall, and utilize encryption.
- Monitor network for intrusion and anomalies 24x7.
- Maintain all software, OS updates and virus signatures.
- Limit Internet usage on computers that process credit cards.
- Only retain information long enough to reconcile payments.
- Shred documentation containing credit card information when it is no longer needed for business or legal reasons.
- Lock computer terminals and paper storage areas when unattended.