Best Practices for Credit Card Processing

- NEVER use e-mail or fax to receive or send credit card data or cardholder data (CHD).
- Only employees who have a legitimate business “need-to-know” should have access to cardholder data.
- Sanitize credit card numbers on any document where the complete number is visible. If necessary to keep other information on the same document, blackout credit card number and then photocopy keeping the copy. Shred the original or send the original to Business Services for processing.
- Cut out/off and shred the CHD.
- Do not enter or store CHD online.
- Do not enter CHD into automated systems for others.
- Eliminate Internet usage on computers or POS systems that process credit cards.
- 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.
- Maintain all software, change passwords regularly.
- 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.
- Monitor network for intrusion and anomalies.