Safeguard the credit card terminal, and any hardcopy cardholder data, when not in attendance.

Examine all credit card terminals regularly to look for possible tampering or substitution (unexpected attachments or cables, missing or changed security labels, broken or differently colored casings, or unknown serial numbers).

Cross-cut shred any hardcopy cardholder data after authorization.

Understand your Incident Response and Continuity Plan, and report any suspected loss of cardholder data to your Payment Card Manager or University Information Security (UIS) Incident Response Team at security@umn.edu.

Record every credit card terminal inspection on your Terminal Inspection Log.

Ensure that you are trained at least annually on how to securely accept and process credit card payments using your credit card terminal.