Store the credit card terminal (and any hardcopy cardholder data) in a locked drawer, cabinet, or safe, when not in attendance.

Examine the credit card terminal upon every use to look for possible tampering (unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings).

Cross-cut shred hardcopy cardholder data after authorization.

Understand your Department Incident Response Plan and report any possible tampering to your credit card terminal, or suspected breach of credit card information, to the University Information Security (UIS) Incident Response Team at (612) 301-4357 or abuse@umn.edu.

Read and understand all University Payment Card Policies and Procedures.

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