Information Security Agreement for Employees Processing Credit Cards

As a credit card handler or processor I agree to abide by the provisions in this document. I have read and will adhere to the Kent State University administrative policy 3342-7-01.2 regarding credit card security.

1. I will complete annual PCI-DSS security training.
2. I will change any initial default password if I have access to a computer or other equipment with credit card processing capabilities.
3. I will utilize sign-in logs, escorts and/or other restrictive measures for all visitors including KSU personnel in areas where cardholder data is handled or maintained.
4. If retaining any cardholder data, it will be clearly marked as confidential and stored securely at all times in a locked drawer or locked file cabinet until no longer needed for business or legal reasons, not to exceed 180 days.
5. I will securely destroy any cardholder data using a cross-cut shredder or a validated record destruction service provider.
6. I will report immediately to my supervisor, the Bursar's Office, and the Office of Security and Access Management any breach or potential compromise of cardholder data. I will use the following methods to notify the appropriate parties:
    a. Supervisor – send email detailing the incident.**
    b. Bursar's Office and Office of Security and Access Management – send email to PCICompliance@kent.edu. **

    **These notifications must not contain any specific cardholder information; those details will be solicited when the incident is investigated.
7. I will never permit unauthorized access to cardholder's credit card information, including but not limited to, the full or partial 16-digit credit card number, expiration date, three (3) or four (4) digit validation code or PIN (personal identification number).
8. I will not transmit or accept cardholder's credit card data by fax or end-user messaging technology such as e-mail, instant messaging, etc.
9. I will not store any electronic cardholder data on a computer file; software, such as an Excel spreadsheet or Word document; server; or portable device such as a laptop, PDA, flash drive, etc.
10. I will never store the three or four digit validation code from the credit card, the Personal Identification Number (PIN) or the magnetic stripe information in any form (written/hard copy or electronic).
11. I will not use an imprint machine to process credit card payments.
12. I will never share a computer password or operator ID if I have access to web-based payment processing.
13. If I am a department head, I have read and agreed that my department will adhere to the requirements of administrative policy 3342-7-01.2, and the Guidelines & Application for Credit Card Acceptance and will complete the annual PCI-DSS self-assessment questionnaire (SAQ) provided by the Bursar's Office for our department.

Employee Name: _____ Campus/ Dept.: _____ Date: _____

Employee Signature: _____ eMail: _____

Manager Name: _____ Manager Title: _____