PCI Signature Form for Illinois State University Employees

Illinois State University employees working with credit cards must read and agree to the following:

A. Approval must be obtained from the eCommerce Committee before entering into any contracts or purchases of software and/or equipment related to credit card processing. This requirement applies regardless of the transaction method or technology used (e.g. e-commerce, POS device).
B. The Department must comply with the Payment Card Industry Data Security Standard.
C. Departmental procedures must be established for safeguarding cardholder information and secure storage of data. This pertains to ALL transactions initiated via the telephone, over the counter, mail order, Internet, etc.
D. Credit card numbers must not be transmitted in an insecure manner, such as by e-mail, instant messaging, unsecured or stored fax (including RightFax or similar networked fax servers), or through campus mail (sealed envelopes must be used).
E. Sensitive cardholder data [i.e., full account number, card type, expiration, PIN, and card-validation code (three-digit or four-digit value printed on the front or back of the card) should not be stored in any University system, personal computer, or e-mail account.
F. The entire credit card number must not be printed on either the department copy or customer copy of any receipts. Old receipts with the entire credit card number should have all but the last four digits blacked out. Do not print the full credit card number under any circumstances.
G. All documentation containing card account numbers must be stored in a secure environment until processed. Secure environments include locked drawers and safes, with limited access to only individuals who are processing the credit card transaction. Processing should be done as soon as possible and the credit card number should immediately be blacked out to the last four digits and the card expiration date must be masked.
H. Stored credit card information will be retained according to the approved document retention policy. All media used for credit cards must be destroyed when retired from use. All hardcopy must be shredded prior to disposal.
I. Background checks must be performed prior to hiring of any positions with access to stored cardholder information.
J. I will not disclose or acquire any information concerning a cardholder’s account without the cardholder’s consent.
K. I will follow all PCI standards.
L. I agree to attend required card security training every year in conjunction with yearly PCI audits.
M. The department has assigned an individual to administer the control of log-in privileges, limit software access to secure locations, delete access to software for terminated employees.
N. I will not use vendor-supplied defaults for system passwords.
O. The complete payment card number is not stored in any third-party software, including cash register systems, and it is prohibited to store complete payment card numbers on University computers at any time.
P. All third parties with access to cardholder data are contractually required to adhere to PCI security requirements and provide proof of PCI certification to the merchant department.

I have read the above and understand Illinois State University’s security policies and procedures.

Printed Name: ___________________________________________________________

Signature: __________________________________________ Date: _______________