RUTGERS
New Jersey Institute for Food, Nutrition, and Health

IFNH POLICY

Category	Content
Policy Name:	Credit Card Terminal Risk Assessment
Section #:	400.4
Section Title:	Financial Management
Approval Authority:	Director of Administration & Finance
Responsible Executive:	Director of Administration & Finance
Responsible Office:	IFNH Business Office
Contact:	Director of Training & Conditioning phone 848-932-0256
Adopted:	05/19/2017
Reviewed:	5/20/2020
Revised:	5/20/2020

1. **Policy Statement**
    a. Proper handling and security of the credit card terminal and associated data both physically and electronically.

2. **Reason for Policy**
    a. This policy fulfills the Payment Card Industry (PCI) requirement to have a written risk assessment for the operation of a credit card terminal.

3. **Who Should Read this Policy**
    a. All individuals associated with the process of accepting and handling credit card payments and / or information.

4. **Resources**
    a. Treasurer's Office: 848-445-2789
    b. Rutgers University Police Department: 732-932-7211
    c. Poynt:
        i. Merchant#: 8030971355
        ii. Voice Auth#: 866-273-0057
        iii. Terminal Support: 877-326-7990
        iv. Merchant Support: 877-326-7990
        v. Supplies: 800-972-7815
    d. Device Name: IFNHPC007
    e. The MID/TID/Bank info:
        i. MID8030971355
        ii. TID0008030971355425
        iii. BankElavon
        iv. Account set up contact at 1-800-725-1243

5. **Definitions**
    a. Devices: Credit Card Terminals

6. **The Policy**
    a. The only types of payment channels that are acceptable for the New Jersey Institute for Food, Nutrition and Health (IFNH) are:

    i. Mail order/telephone orders (MOTO)
    ii. Card-present (face-to-face)
    iii. Fax orders
b. Types of payment channels that are NOT ACCEPTABLE:
    i. Email orders (because they are considered not secure)
c. The credit card terminal is to only be connected to RUWireless Secure.
d. Cardholder information is not to be stored in electronic format by IFNH.
e. If IFNH does store cardholder information it can only be in paper reports.
f. All manufacturer default terminal and online accounts if applicable must be deactivated at all times or removed from the system.
g. All transactions are processed with payment encryption and tokenization.
h. All firmware updates are pushed down to the terminal by the payment processing provider as they become available.
i. Access to the credit card terminal and cardholder data is to be limited to only those individuals with a legitimate business need to have access.
    i. Individual's access is based on their job classification and function.
j. Access to the cabinet were the credit card terminal is stored (locked) is controlled by a card reader control access system. This system records who accesses the floor by time and day. The cabinet the credit card terminal is stored in is always locked with the Director for Training & Conditioning possessing the key. There is another key stored in the key lock box which is locked away in a separate cabinet on the floor.
k. The building and the floor in which the credit card terminal are stored are under 24/7 video camera surveillance.
l. Both the card control access system and video surveillance are protected from tampering or disabling.
m. We will use a cross-cut shredder to shred all hardcopy materials in regards to this business process. The shredder we use shreds 12 sheets per pass into 5/64"x 5/16" micro-cut particles (Security Level P-5).
n. A list of all devices that capture payment card data will be maintained in the IFNH Business Office, updated when a new device is acquired, relocated and/or decommissioned, and will include the following information:
    i. Make & model of device
    ii. Location of the device (room & address)
    iii. Unique Identifier (e.g. serial number)
o. On a monthly basis the devices that captures payment card data are to be inspected for tampering or substitution.
p. Personnel are trained to be aware of suspicious behavior and to report tampering or substitute devices.
q. Personnel are required to verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot any device.
r. Personnel are required to verify any installation, replacement or return of devices.
s. All entries are recorded with User Identification, Type of Transaction, Date & Time, and Success or Failure Indication.
t. A list of all personnel with approved access to the devices are to be maintained in the IFNH Business Office.
u. It is the responsibility of all personnel with access to keep and maintain all information in a secure manner.
v. The devices are to only be used on Rutgers University premises.
w. If a security situation occurs personnel are to report it to the IFNH Business Office who will then report the situation to the necessary Rutgers University authorities including but not limited to the Treasurer's Office and Rutgers University Police Department.
    i. The following information is to be reported if a situation should occur:

1. The roles and responsibilities of personnel involved.
2. Date and Time
3. Transaction information involved including:
    a. Date
    b. Time
    c. Payment Type
    d. Nature of Compromise

x. User identification and passwords to all system areas are to be maintained securely.
y. A special password is necessary to enact refunds/credits in the system.