Merchant Card Processing Request Form

NORTHWESTERN UNIVERSITY

This form must be filled out completely, reviewed, vetted and approved before any new NU Merchant location accepts credit card payments via manual/electronic terminal or e-Commerce application (e.g. Virtual Terminal, Web, Point-of-Sale or Cloud). Completion of this form is also required if architecture and/or scope of an NU Merchant's existing payment applications changes.

Date of Application: _____ Type of Request: ☐ e-Commerce ☐ Manual Terminal

1. Dept. Name _____ Dept. Phone # _____ Dept. Fax # _____
   Dept. Bldg/ Street _____ City _____ Zip Code _____ Mail Code _____

2. Business Contact
   Name _____ Phone # _____ email _____

3. Account Number to charge for monthly rental and discount fees _____
   Fund (3 digits) – Department (7 digits) – Project (8 digits, optional) – Activity (2 digits, optional) – Account (5 digits, usually 78680)

4. Billing information (if different than above):
   Billing Name _____ Billing Phone # _____ Billing Fax # _____
   Billing Bldg/ Street _____ City _____ Zip Code _____ Mail Code _____

5. A location name must begin with with "NU <space>" and be followed by no more than 20 additional characters, including spaces, for a maximum 23 characters total. *The location name will print as the description on the customer credit card statement.* Choose a name that your customer will recognize.
   Example location name: NU Department Store
   Requested location name: NU

6. Attach documentation signed by the Director of the Department and the Business Manager of the school:
   - ☐ Project description: business purpose, services and products being sold, project plan including timeline
   - ☐ Estimated annual transaction volume and average dollar amount per transaction
   - ☐ e-Commerce Application Addendum (for e-commerce requests only)
   - ☐ Procedures for collecting, recording, and reconciling sales and refunds (including cash, checks, and charges).
     - ☐ **ATTACH SEGREGATION OF DUTIES MATRIX** – Must Include specific staff and/or positions responsible for process steps ensuring duty segregation, and independent review and reconciliation of transaction data.

In signing, the authorizing parties confirm that:

- All impacted personnel have read the NU Merchant Card Processing Policy and agree to adhere to it.
- The department agrees to participate in the Treasury Operations administered PCI compliance programming including completing annual questionnaires and attending security training and informational meetings.

Requested by:		Director or Dean Approval:	
Printed Name	_____	Printed Name	_____
Title	_____	Title	_____
Signature	_____	Signature	_____
Date	_____	Date	_____

Please return to e-Commerce Operations, 619 Clark St., Room 110, Evanston Campus MC 1130 CCard@northwestern.edu
MERCHANTS CANNOT ACCEPT CHARGES WITHOUT APPROVAL FROM E-COMMERCE OPERATIONS.

NORTHWESTERN UNIVERSITY

e-Commerce Application Addendum

This form must be attached to the Merchant Card Processing Request Form.

The following information must be provided when requesting to process credit cards over the internet.

A. Proposed URL: _____

B. **Department's Technical Contact** (Usually differs from the Business Contact on the main application form)

Name _____ Phone # _____ email _____

C. Select type of e-commerce system proposed and relationship of **Third Party Service Provider (TPSP/Vendor)** to application ownership, architecture, hosting and responsible parties

☐ The e-Commerce, POS or Virtual Terminal system is both hosted and maintained by an offsite **TPSP/Vendor** (if **Virtual Terminal** – please contact e-Commerce Operations for assistance)

TPSP/Vendor name: _____

Software Application name: _____

Payment Processor/Gateway name (i.e. Payflow Link, Authorize.net, etc.): _____

Name and email address of **TPSP/Vendor Technical Lead** (required by NU and Card Issuers): _____

System is/will be ☐ **Owned** or ☐**Leased**

☐ Department-hosted **TPSP/Vendor** software application, payment processing outsourced

TPSP/Vendor name: _____

Software Application name: _____

Payment Processor/Gateway name (i.e. Payflow Link, Authorize.net, etc.): _____

Name and email address of **TPSP/Vendor Technical Lead** (required by NU and Card Issuers): _____

System is/will be ☐ **Owned** or ☐**Leased** _____

☐ Department-hosted, **Custom Developed (internally built)** application software, PayPal Payflow Pro, Payflow Link or other gateway for payment processing

Describe Application **in Detail**: _____

Payment Processor/Gateway name (i.e. Payflow Link, Authorize.net, etc.): _____

Name and email address of **Custom Application Responsible Party** _____

Please return to e-Commerce Operations, 619 Clark St., Room 110, Evanston Campus MC 1130 CCard@northwestern.edu
MERCHANTS CANNOT ACCEPT CHARGES WITHOUT APPROVAL FROM E-COMMERCE OPERATIONS.

For all YES answers below, evidence is required and must be attached.
For all NO answers below, explanations are required and must be attached.
ALL Proposals and Contracts are subject to additional review and vetting.

D. Are all vendors, service providers, hosts and gateways verifiably **PCI compliant**?
☐ Yes ☐ No

E. Are all vendors' and service providers' *payment applications* **PA-DSS compliant**?
☐ Yes ☐ No

F. Are all **Vendor/TPSP proposals and/or countersigned (executed) contracts** attached?
☐ Yes – Proposals are Attached
☐ Yes – Countersigned (Executed) Contracts are Attached
☐ No – Neither Proposals nor Countersigned (Executed Contracts) are Attached

G. Do all **Vendor/TPSP proposals and/or countersigned (executed) contracts** clearly specify and itemize details of scope of service, materials (hardware and software), support, relationship and liability between primary **Vendor/TPSP** and any **nested Vendor/TPSPs** whose services have been included in the processing solution?
☐ Yes – Itemization as Specified is Included in the proposals and/or countersigned (executed) contracts
☐ No – Itemization as Specified is not included in the proposals and/or countersigned (executed) contracts

H. Do all **Vendor/TPSP proposals and/or countersigned (executed) contracts contain NU PCI-specific Data Security Agreement and Liability Shift language** pursuant to PCI DSS requirement 12.8 and NU requirements?
☐ Yes ☐ No

I. Is **TPSP-supplied diagram of the TPSP's application, processing, gateway, security and network architecture** which supports and all interaction with the CDE (Cardholder Data Environment) outside and inside of NU attached?
☐ Yes ☐ No

J. Is **NUIT-supplied Network diagram depicting the architecture and security of all on-campus computing assets that will be connected to the proposed system and CDE** (Cardholder Data Environment) attached?
☐ Yes ☐ No

K. **Will department personnel view or enter cardholder data** (i.e. entering purchases on behalf of customers, processing refunds based on card number, or generating reports that include card numbers)?
☐ Yes ☐ No

L. If Yes, **have these employees had background checks performed by Human Resources**?
☐ Yes ☐ No

M. **Will CHD (Cardholder Data) be stored, processed or transmitted on equipment or systems connected to the NU network**?
☐ Yes ☐ No

.

FOR E-COMMERCE OPERATIONS USE
Notes/Comments on Documentation attached:

☐ Evidence of **Vendor/TPSP PCI Compliance**
_____
☐ Evidence of **Vendor/TPSP Payment Application PA-DSS Validation**
_____
☐ **Vendor/TPSP proposals and/or countersigned (executed) contracts**
_____
☐ Proposals/Contracts **contain Itemization and specification, liability and relationships, plus any nested Vendor/TPSPs**
_____
☐ TPSP-supplied diagram of the TPSP's application, processing, security and network architecture which supports and all interaction with the CDE that will be connected to the proposed system
_____
☐ NUIT Network diagram depicting all on-campus computing assets that will be connected to the proposed system
_____

Please return to e-Commerce Operations, 619 Clark St., Room 110, Evanston Campus MC 1130 CCard@northwestern.edu
MERCHANTS CANNOT ACCEPT CHARGES WITHOUT APPROVAL FROM E-COMMERCE OPERATIONS.

Merchant Card Request Administrative Record

For Treasury Operations and e-Commerce Operations Office Use Only

LOCATION NAME _____

DATE REGISTERED _____

NU LOCATION CODE _____

AMEX MERCHANT # _____

VMCD MERCHANT # _____

PAYPAL ID _____

CARD PROCESSING TYPE ☐ e-Commerce ☐ Terminal ☐ Other

MERCHANT LOCATION PCI ANNUAL QUESTIONAIRE TYPE

☐ **SAQ A v.3.0** ☐ **SAQ A-EP v3.0**

☐ **SAQ B v.3.0** ☐ **SAQ B-IP v.3.0**

☐ **SAQ C v.3.0** ☐ **SAQ C-VT v.3.0**

☐ **SAQ D v.3.0** ☐ **SAQ P2PE-HW v.3.0**

MERCHANT LOCATION PCI ANNUAL SCAN REQUIRED ☐ **Yes** ☐ **No**

URLs and IP Addresses Impacting the Cardholder Data Environment TO BE SCANNED:

For e-commerce requests:
NUIT has reviewed the department's security policies, contracts, and e-commerce system environment and approves of the security measures in place.

David Kovarik, Director
Director of Information & Systems Security/Compliance
Date

Robert Gabella
e-Commerce Program Supervisor
Date

Richard Emrich
Director of Treasury Operations
Date

Nancy Pinchar
Assistant Controller
Date

Merchant Onboarding Checklist

Prior to the first card swipe or online transaction, the following must be completed:

Requirement	Responsible Party	Name	Date Completed
Provide names, email addresses and titles of all staff of the Merchant Processing operation (use the table, following page)	Department Manager/ Business Lead		
Attach completed departmental Merchant Processing Policy document include Segregation of Duties (SoD) Matrix (sample following page)	Department Manager/ Business Lead		
Mandatory review of NU PCI DSS Program and Policies	All Department Staff from list below		
Mandatory NU online PCI Security Awareness Training and Attestation	All Department Staff from list below		
TPSP (Vendor) Mandatory NU online PCI Security Awareness Training and Attestation – for any personnel interacting with or configuring the CDE	Department Manager/ Business Lead		
Secure AMEX and Processor/VMDC MIDs, TIDs and DIDs as Required	e-Commerce Supervisor or e-Commerce Analyst		
Optional: Secure PayPal PayFlow Link or Pro account (if Required) and set up users/roles as Required	e-Commerce Supervisor or e-Commerce Analyst		
Add new merchant to TrustKeeper Portal and send notification to Department Manager	e-Commerce Supervisor or e-Commerce Analyst		
Complete Merchant Enrollment questionnaire on TrustKeeper Portal	Department Manager/ Business Lead/ IT Staff		
Complete initial Merchant PCI Self-Assessment Questionnaire on TrustKeeper Portal	Department Manager/ Business Lead / IT Staff		
For e-Commerce Merchants, set up TrustKeeper and/or NUIT Vulnerability scan schedule and scan parameters – in TrustKeeper Merchant Portal	Department IT Staff with e-Commerce and/or NUIT Security and Compliance Personnel		

Merchant Onboarding Checklist - Continued

In the table below, please list the names and email addresses of all **Departmental Staff** that will be part of the new NU Merchant card operation. The list should include all staff that will be involved in the credit card operation regardless of status. Each applicable **Staff Member** is required to:

1. Review the PCI Security Policy
2. Participate in an annual PCI-DSS Security Awareness Training
3. Attest after completing both items above using the instructions provided in item 1

Name	Email Address	Title/Role or Function

In the table below, please list the names and email addresses of all **TPSP (Third Party Service Provider/Vendor) Staff** that will be part of the new NU Merchant card operation. The list should include all staff that will be involved in the credit card operation, integration, testing or support regardless of status. Each applicable **TPSP (Third Party Service Provider/Vendor) Staff Member** is required to:

1. Review the NU PCI Security Policy
2. Participate in an annual NU PCI-DSS Security Awareness Training
3. Attest after completing both items above using the instructions provided in item 1

Name	Email Address	Title/Role or Function

Merchant Card Processing Procedures

For Use in Developing/Amending a Departmental Operations Manual

Purpose of This Guide

The following processing procedures are presented to highlight security procedures and segregation of duties in a payment receiving operation for a credit card terminal based environment. **Segregation of duties (SoD)** is a key concept of internal controls wherein having more than one individual complete a set of tasks is a requirement and is intended to prevent error and fraud. Use this as guide when completing the **item 6** addendum (Procedures for collecting, recording, and reconciling sales and refunds…) of the Merchant Card Processing Request Form. In addition, the **SoD Matrix** on the last page of this guide must be completed and accompany the addendum to the **Merchant Card Processing Request Form**.

NOTE: If a department does not have adequate resources to demonstrate proper duty segregation, at the very least, there must be proper oversight by a supervisor, manager, or business administrator who reviews and approves (signed or initialed, and dated) the work of the staff performing the assigned duties. In such cases, this should be clearly noted in the addendum and departmental policies, and reflected appropriately in a completed **SoD Matrix**.

Daily Procedures

For the use of Point of Sale terminals, Virtual Terminals, or Virtual Terminal administrative functions of e-Commerce Applications– the following procedures must be clearly elaborated upon, specific to the unique environment of each NU Merchant Location (some may also apply to phone line connected terminals).

- State clear register **opening and closing procedures which would center on unique Windows, then Application level, login and password** for each cashier; supplement with cash drawer building and opening procedures performed by Manager.

- State clear procedure for **securing register/terminal when stepping away from it for any reason** (is there a "secure" mode – for example – in the proposed application, that requires cashier user ID and password before proceeding with next use?).

- State clear procedure for **securing register/terminal after business hours**

- Can multiple cashiers work off the same register and drawer if properly logged in (in other words – does the proposed system issue an audit trail for **EACH** transaction?)
    - **Whether yes or no**, the policy must state clearly that additional cashiers (or even a manager) **may not be permitted to** use a register or terminal with another cashier's user credentials.

- Can transactions be suspended and reopened?
    - **If yes or no** – what is the procedure to move to the next customer in line if the current customer presents a purchase after they forgot their money or card, and requests to return after retrieving?

- End of shift routines surrounding Z/ZZ and other activity reports generated by the e-Commerce, POS or VT system (either on receipt printer or remotely) , as well as drawer close-out, must be clearly spelled out – at what point and with which tasks does the cashiering role end and the managerial/supervisory role begin?

- **Specify procedures for inspecting card, matching digits, verifying signature and other Card Issuer Required steps** http://usa.visa.com/merchants/protect-your-business/fraud-control/card-present.jsp

Daily Activity Processing

- **Staff member A** receives credit card payments (card-present or card-not-present) throughout the day and runs payments through the credit card swipe terminal
- **Staff member A** adds up all merchant slips by card type at the end of the day and forwards the merchant slips with the totals by card type to **staff member B**.
- **Staff member B** extracts a ***card totals report of the day's activity*** from the credit card terminal and compares the totals to the totals of the merchant slips to ensure a match.
- **Staff member B** settles the batch if totals match and a batch settlement report is generated. In cases where batches are allowed to settle automatically, reports should be cross-referenced and any variances between the settlement report and the card totals report must be noted and immediately reported to Depository Services for investigation.
- S**taff member A** creates the deposit using the CRT (Cash Receipt Ticket) module in PeopleSoft Financials if no variances are found
- **Staff member C** (if the role/resource exists, otherwise staff member B) commits the CRT
- **Any staff member** files copies of daily activity processing documents including card totals report, batch settlement report and copies of the CRT for the appropriate amount of time per the standard document retention guidelines (3 fiscal years in addition to the current year)

Delinquent Deposits (when applicable)

- If any CRTs have not been created for an extended number of days, Depository Services contacts **staff member A** to create the deposit
- **Staff member A** creates the CRT
- **Staff member C** (if the role/resource exists, otherwise staff member B) commits the CRT

Refunds/Credits (when applicable)

Any refunds processed are also reflected in the reports ran during the course of daily activity processing.

- Refund requests are received by **staff member A** and forwarded along with any substantiating documentation to a **supervisor** or **manager** for approval
- Upon approval, **staff member A** processes the refunds using the terminal

Weekly Procedures (when applicable)

Delinquent Deposits

If any outstanding deposits have not yet been created and/or committed, **Depository Services staff** submits a letter with details pertaining to any unprocessed CRTs to the **department manager/supervisor**.

- Department manager or supervisor directs **staff member A** to create/commit the outstanding deposits

NOTE: DELINQUENT DEPOSIT REPORT IS SUBMITTED TO NU INTERNAL AUDIT AND ADVISORY SERVICES WEEKLY

Monthly Reconciliation/Review

Budget Statement Review

- **Department manager** or **supervisor** reviews budget statements monthly against backup documents to confirm that all daily transactions for the month tie out to the budget reports on a month by month basis and credits have proper approval.
- On a monthly basis, the department receives a statement of merchant card processing fees from Depository Services. The **department manager** or **supervisor** verifies that any fees incurred match the amounts on both the merchant card processing statement and the journal voucher processed by Depository Services.

Resources

1. The following classes offered by the **Office of Human Resources Workplace Learning** might be helpful to departments or staff new to the University business environment and framework for compliance:
2. HRD700 – Introduction to University Business Processes (Online)
   HRD705 – Effective Business Operations

SoD (Segregation of Duties) Matrix EXAMPLE ONLY

This grid should help evaluate whether assignments provide appropriate segregation of duties and oversight. They should align with Roles A, B, C (if available), and supervisor or manager.

Position/Staff	Receive and/or process payments *	Run end-of-day reports of daily activity	Review daily sales	Account, reconcile and balance daily credit card transactions	Batch/close out daily credit card transactions	Prepare deposits (CRTs)	Commit CRTs	Approves assigned tasks	Process refund requests	Approve Refunds	Monthly reconciliation of budget statements against departmental records
Staff Member A or Automated (if e-Commerce)	X				X						
Staff Member B: NAME, role	X	X							X		
Staff Member C: NAME, role			X			X			X		
Staff Member D: NAME, role				X			X	X		X	X
For the purpose of this example, Staff Member B is either an a Cashier/First Line Employee, C is a Manager or Staff Member, D is a Supervisor, Department Head or Dean											

SoD (Segregation of Duties) Matrix EDITABLE

Position/Staff	Receive and/or process payments *	Run end-of-day reports of daily activity	Review daily sales	Account, reconcile and balance daily credit card transactions	Batch/close out daily credit card transactions	Prepare deposits (CRTs)	Commit CRTs	Approves assigned tasks	Process refund requests	Approve Refunds	Monthly reconciliation of budget statements against departmental records

Instructions:

1. Complete the above matrix by **entering the positions and names of staff members** designated to perform the duties in the first column
2. **If more than one staff member is assigned per duty, enter separate lines for each staff member**
3. **CLICK INSIDE THE CELL** that corresponds to the staff member's duties and a check mark will appear.