

IT checklists for Columbia University e-commerce websites

This document contains 3 checklists for three different types of e-commerce websites permissible under University e-commerce policy. These checklists should be used to ascertain that Columbia University websites with e-commerce components conform to the University’s policy. For more information about this document or e-commerce policy in general please email *creditcards@columbia.edu*

1. Columbia e-commerce sites hosted INSIDE Columbia University 2

2. Columbia e-commerce sites hosted OUTSIDE Columbia University 4

3. Columbia application service provider websites with an e-commerce component that are hosted OUTSIDE Columbia University 6

IT checklists for Columbia University e-commerce websites

1. Columbia e-commerce sites hosted INSIDE Columbia University

This checklist is for situations wherein the merchant website is hosted on the Columbia University computer network.

University Policies: You should be familiar with the University's E-commerce policy and how it affects your work in this area.

SSL Certificate: If your site allows registration, serves any kind of shopping cart page(s), serves forms that accept name, email address and/or other personal information, or displays subtotal/total cost of merchandise, these pages **must** be served securely using an SSL certificate. Please provide the URL for your website for us to review.

[http://]

Online Payment Form: Columbia's policies clearly state that no online payment forms may be served from a University server or from the University network. You must establish a relationship with an approved third-party provider of e-commerce services such as global payments, cybersource, etc. and serve your payment form(s) from their domain and their servers. Please provide either the URL for the payment page or the URL for the page on your website that contains the link that will re-direct visitors to the future payment page.

[http://]

Privacy Policy: Every website with an e-commerce function must contain a privacy policy page and links to that page from throughout the site. In order to receive a **MID**, you must provide the URL to your privacy policy page. Please provide the URL for the privacy policy page.

[http://]

IT checklists for Columbia University e-commerce websites

Refund Policy: Every website with an e-commerce function must contain a refund policy page and links to that page from throughout the site. In order to receive a *MID*, you must provide the URL to your refund policy page. Please provide the URL for the refund policy page.

[http:// _____]

MID/PIN visibility: In the course of building the 3rd-party hosted payment form, the developers must make certain that CU-issued Merchant ID and/or CU vendor-issued PINs are NOT visible anywhere in the source code of the form. Please provide the URL to the payment page so we may view the page source.

[http:// _____]

IT checklists for Columbia University e-commerce websites

2. Columbia e-commerce sites hosted OUTSIDE Columbia University

This checklist is for situations wherein the merchant website is developed by a Columbia employee or a vendor hired by a Columbia employee, but hosted somewhere outside the Columbia network.

University Policies: You should be familiar with the University's E-commerce policy and how it affects your work in this area.

If your website is being hosted at a PCI-compliant hosting facility on PCI-compliant infrastructure you will be permitted to keep your payment page(s) integrated with your website (see item 4 below.) In this case, you will need to procure written documentation from your website hosting vendor that all the requirements of PCI-DSS compliance are met for your website. If your 3rd-party hosting vendor is not providing PCI-compliant hosting, then you will need to separate your payment page(s) from the rest of your website as explained below.

SSL Certificate: If your site allows registration, serves any kind of shopping cart page(s), serves forms that accept name, email address and/or other personal information, or displays subtotal/total cost of merchandise, these pages **must** be served securely using an SSL certificate. Please provide the URL for your website for us to review.

[http://]

Online Payment Form: Columbia's policies clearly state that no online payment forms may be served from a University server, from the University network or from non-PCI-compliant 3rd-party servers or infrastructure. If your 3rd-party hosting vendor provides written documentation that your

IT checklists for Columbia University e-commerce websites

site is being hosted on PCI-compliant infrastructure, then you may elect to keep your online payment form integrated with the rest of your website. If not, you must establish a relationship with an approved third-party provider of e-commerce services such as global payments, cybersource, etc. and serve your payment form(s) from their domain and their servers. Please provide either the URL for the payment page or the URL for the page on your website that contains the link that will re-direct visitors to the future payment page hosted on an approved vendor's PCI-compliant web infrastructure.

Privacy Policy: Every website with an e-commerce function must contain a privacy policy page and links to that page from throughout the site. In order to receive a *MID*, you must provide the URL to your privacy policy page. Please provide the URL for the privacy policy page.

[http://]

Refund Policy: Every website with an e-commerce function must contain a refund policy page and links to that page from throughout the site. In order to receive a *MID*, you must provide the URL to your refund policy page. Please provide the URL for the refund policy page.

[http://]

MID/PIN visibility: In the course of building the payment form (whether it's integrated with your website or hosted by an approved PCI-compliant vendor), the developers must make certain that CU-issued Merchant ID and/or CU vendor-issued PINs are NOT visible anywhere in the source code of the form. Please provide the URL to the payment page so we may view the page source.

[http://]

3. Columbia application service provider websites with an e-commerce component that are hosted OUTSIDE Columbia University

This checklist is for situations wherein a Columbia merchant is using a 3rd-party web-based application service provider and the website is hosted outside the Columbia network.

University E-Commerce policy: You should be familiar with the University's E-commerce policy and how it affects your work in this area.

Your vendor, the provider of the web-based application/service that you are contracting them for must provide written documentation that their application, and the infrastructure which serves it, meets all aspects of PCI-DSS compliance. You should do this *BEFORE* you sign an agreement to contract services from them. If your website application service provider *cannot* or *will not* provide written documentation that their application and the infrastructure which serves it meets all aspects of PCI-DSS compliance, then you will need to separate your payment page(s) from the rest of your website as explained below.

SSL Certificate: If your web application allows or requires registration, serves any kind of shopping cart page(s), serves forms that accept name, email address and/or other personal information, or displays subtotal/total cost of merchandise, these pages *must* be served securely using an SSL certificate. Please provide the URL for your website for us to review.

[http:// _____]

Online Payment Form: Columbia's policies clearly state that no online payment forms may be served from a University server, from the University network or from non-PCI-compliant 3rd-party servers or infrastructure. If your 3rd-party application service provider does not provide written documentation that all aspects of your web application are PCI-compliant and hosted on PCI-compliant infrastructure, you must establish a relationship with an approved third-party provider of e-commerce services

IT checklists for Columbia University e-commerce websites

such as global payments, cybersource, etc. and serve the payment form(s) of your web application/service from their domain and their servers. Please provide either the URL for the payment page or the URL for the page on your website that contains the link that will re-direct visitors to the future payment page hosted on an approved vendor's PCI-compliant web infrastructure.

[http:// _____]

Privacy Policy: Every website with an e-commerce function must contain a privacy policy page and links to that page from throughout the site. In order to receive a *MID*, you must provide the URL to your privacy policy page. Please provide the URL for the privacy policy page.

[http:// _____]

Refund Policy: Every website with an e-commerce function must contain a refund policy page and links to that page from throughout the site. In order to receive a *MID*, you must provide the URL to your refund policy page. Please provide the URL for the refund policy page.

[http:// _____]

MID/PIN visibility: In the course of building the payment form (whether it's integrated with your website or hosted by an approved PCI-compliant vendor), the developers must make certain that CU-issued Merchant ID and/or CU vendor-issued PINs are NOT visible anywhere in the source code of the form. Please provide the URL to the payment page so we may view the page source.

[http:// _____]