UBC ePayment Web Service provides participating UBC departments with secure, real-time authorization and processing of credit card and/or Interac Online® payments. As with other payment processes on campus, ePayment is subject to UBC ePayment PCI DSS compliancy, which merchants must be compliant with at all times.

**Credit Card Security:**

# A.

* ePayment Web Service merchants are not permitted to obtain, collect or store sensitive credit card information.
* ePayment Web Service merchants are not permitted to process payments on the behalf of their customer or the cardholder.
* ePayment Web Service merchants are subject to training sessions and audits to ensure PCI DSS compliancy
* Please refer to the UBC ePayment PCI DSS compliancy requirements available at https://epayment.it.ubc.ca for the full list of restrictions and requirements.

Multi-currency credit cards are accepted but ePayment transactions are posted and booked in CAD currency only

To comply with British Columbia’s Freedom of Information and Protection of Privacy Act (FIPPA) and UBC Information Security Standards, new Web Service merchant requests have to complete Privacy Information Assessment (PIA) review. Existing web forms needing changes on the manner/process of collecting user information on their web forms may also require PIA review. Details of the PIA process may be found here: <https://privacymatters.ubc.ca/pia-process-overview>

## Please provide:

|  |  |  |  |
| --- | --- | --- | --- |
| **Department/Organization/Unit** | | Required |  |
| **Merchant Name –** name to be displayed for merchant on CBM Admin | |  |
| **Provided Services –** name of item to be displayed on customer receipt | |  |
| **Operational Contact email (**for payment inquiries e.g., finance/admin clerk, others) | |  |
| **Business Contact**  (someone who oversees the payment operations) | **Name** |  |
| **Email** |  |
| **Technical Contact**  **(**for system maintenance and releases) | **Name** |  |
| **Email** |  |
| **GL code**. **–** default value   * **FMS Chart field codes (not WorkDay)** should **not** have ‘R’ or ‘Grant permitted’ **nor** ‘E’ or ‘Gift permitted’values * Account Number should start with ‘**4**’ (but cannot be 499999, grant, or research revenue) | | |  |  | | --- | --- | | Fund Code |  | | Dept Code |  | | Program (optional, **5 characters**) |  | | Project ID |  | | Account Number |  | |
| **ePayment Worktag (**from WorkDay) | |  |
| **Service Provider** – identifies the web service provider e.g., ePly, Web Services, CMS, etc. | |  |
| **Will the information collected by your shopping cart/registration system be stored within UBC? If not, please specify country. If it is outside of Canada, please read below.** | |  |
| According to Canadian privacy law, storage of personal information outside Canada is prohibited, unless consent is given. Thus **if the information is stored outside Canada**, **then your shopping cart/registration system must have a privacy clause statement checkbox prior to payment checkout.** Below is an example:  cid:687DA2E8-4E10-4103-A125-1AA68F42E851 | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Expected Go Live date** | | Optional |  |
| **Expected Periods of Activity** | |  |
| **Department/Organization/Unit Web Site URL** | |  |
| **Shopping cart URL –** if already available/existing | **Test** |  |
| **Prod** |  |

**Declare and Submit**

|  |  |  |
| --- | --- | --- |
| I/We do hereby confirm (mark boxes below):   * That this request is for/on behalf of a UBC Entity * That payments or fees to be collected for this merchant is for a UBC-related activity * As owner/overseer of this merchant account, to comply with the following requirements * UBC data privacy and information security e.g., **https://privacymatters.ubc.ca/pia-process-overview** * Adherence to UBC ePayment PCI DSS mandates, please see **ePayment PCI Compliance Training** * British Columbia’s Freedom of Information and Protection of Privacy Act (FIPPA) and UBC Information Security Standards     That I/we confirm acceptance of the terms of this declaration  I/We confirm that I/we have a plan in place, to address the security and privacy risks identified by the PIA  assessment | | |
| **Date** | **Requested by -** Name | Signature |
| **Date** | **Approved by -** Name | Signature |