UNIVERSITY OF BRITISH COLUMBIA
WEB ACCESS TO FINANCIAL MANAGEMENT INFORMATION SYSTEM
SECURITY ADMINISTRATOR APPLICATION FORM

IDENTIFICATION

First Name:	Last Name:
Department:	Email Address:
Employee ID:	Telephone:
CWL ID*:	
Signature **	Date

*** Requestor must have access to FMS nQuery before applying for security administrator access.**
**** I acknowledge and accept the terms of use as defined by University policy and by the attached non-disclosure agreement**.

AUTHORIZATION TO GRANT SECURITY ADMINISTRATOR ACCESS PRIVILEGE FOR THE FOLLOWING FMIS DEPARTMENT IDS

APPROVAL BY DEAN OR DEPARTMENT HEAD

Authorised by:	Title:	
Print Name:	Telephone:	Date / /

FOR FINANCIAL SERVICES AUTHORIZATION ONLY

Date / /	Signature	Comments

FOR FINANCIAL SERVICES SECURITY ADMINISTRATOR ONLY

Completed / /	Initials	Comments

FAX to 604-822-2417 (c/o Data Management) or scan the form and send in an email to peoplesoft.support@ubc.ca ***Note****: if the form is faxed or emailed please do not send the original as well.*

If there are any questions regarding this form or other PeopleSoft security please send an email to peoplesoft.support@ubc.ca

Non-Disclosure Agreement

Financial records available from the Financial Management Information System (FMS) are confidential and the Property of the University of British Columbia.

Data security of the FMS system is defined as the protection of information systems, data facilities, and resources against accidental or deliberate threats to their confidentiality, integrity, or availability.

Deans, Directors and Department Heads are accountable for ensuring the responsible use of administrative system access privileges granted through their authority. Specifically, individuals authorizing administrative system access are responsible for:

- Ensuring that the level of access authorized is sufficient and necessary;
- Ensuring that faculty, staff and students granted access privileges under their authority are aware of this security agreement and accept individual accountability and responsibility for use or abuse of granted system privileges.

Information end users are responsible for the prudent and secure use of information facilities in compliance with good business practice and security standards. An information end user assigned a unique user identification code and secret password is individually accountable for all systems access granted through that user identification code and password. End user responsibilities include, but are not limited to:

- The protection of individual user identification codes and associated passwords;
- Ensuring that workstations are not left unattended;
- Ensuring that sensitive information displayed on end user workstations or hard-copy reports is not visible to unauthorized individuals;
- Ensuring that this security agreement is not violated by the use of the individual identification codes by or at another end user.

Protection of information assets and compliance with this security agreement and accompanying procedures are basic terms of continued administrative system access privileges. Failure to comply with this agreement could result in disciplinary action including termination of system access privileges.

The request will be reviewed and authorized by Financial Services. Once completed, you will receive an e-mail notification.

If you require assistance, please contact *peoplesoft.support@ubc.ca*