



Learning Management Systems (LMS) Administrative Access and Confidentiality Agreement

Background:

UBC IT has recently updated the Information Security Manual and issued guidelines for handling Personally Identifiable Information (PII).—Staff who provide instructional support have access to considerable PII. As a result of these changes, and consistent with best practice, administrative access to the LMS now requires an authorized access form and completion of a confidentiality statement.

As UBC Policies, Security Guidelines and legislation change, we will inform you of alterations to the terms and conditions of access, as applicable.

Instructions:

1. Please fill in your contact information and requested role.
2. Please read the guidelines outlined in this document and the related policies outlined in this document.
3. Sign the form.
4. Obtain approval from your Department Head/Program Director and Faculty Dean/Director/Principal.
5. Please scan your completed form and email to lt.hub@ubc.ca with your request for access.
6. UBC IT will review the request and confirm your access.

Contact Information:

Name/CWL ID: _____

Department: _____

Position: _____

Email: _____

Phone: _____

engage • envision • enable



Learning Management System Confidentiality Statement

The LMS system (currently, Blackboard *Connect*) contain confidential and/or sensitive information. For example:

- **Faculty and/or Staff Member:** PUID/student number, first name, last name, email address
- **Teaching Assistant:** student number, first name, last name, employee ID, PUID, email address
- **Student:** student number, first name, last name, email address, enrolment

Some of this information is Personally Identifiable Information (PII), which is subject to the BC *Freedom of Information and Protection of Privacy Act* (FIPPA). Under section 30 of FIPPA, UBC has an obligation to protect personal information from unauthorized access, collection, use, disclosure or disposal. For further information on FIPPA, please see the Office of the University Counsel website at <http://universitycounsel.ubc.ca/information-and-privacy/>.

All of the information is also subject to the following UBC Policies, which you are responsible for reading:

- UBC Policy 104 Accessible Use and Security of UBC Electronic Information Systems
<http://universitycounsel.ubc.ca/files/2013/06/policy104.pdf>

Under the above Policies, you are also required to comply with UBC's Information Security policies at: <https://it.ubc.ca/services/security/ubc-information-security-office/security-policies>

In particular, users should take responsibility in meeting the [User Standards](#) and [Management and Technical Standards](#) outlined in the UBC's Information Security Standards at: <https://cio.ubc.ca/information-security/policy-and-standards>



Learning Management System Administrative Access Form

Access Level:

**Faculty or
Department(s)**

Role:

ISS System Administrator

- Access courses for specified faculty or department/program without being enrolled in each course.
- Modify course properties such as availability, duration, and course name for specified faculty or department/program.
- Manage enrollments for specified faculty or department/program.
- Manage course content such as copying course content from one course to another and reset courses for specified faculty or department/program.
- Create Courses (within certain restrictions) for specified faculty or department/program.

IT Service Desk

- View user enrollments system-wide.
- View course properties such as availability, duration, and course name for specified faculty or department/program. Note: Due to application constraints, this role provides the ability to manage course properties. Per this agreement, properties should only be viewed.



Learning Management System Confidentiality Agreement

1. I understand that I am responsible for the confidentiality and security of all confidential or sensitive information that I am able to access in the Learning Management System(s). I will:
 - (a) Only access, use and alter the Information as authorized in the Systems Access Level section of this form; and,
 - (b) Refrain from sharing the Information with unauthorized users.
2. When I access the Information using a computer or mobile computing device, I will take reasonable steps to ensure that unauthorized users are unable to view the Information.
3. When I extract, download, print or summarize the Information, I will:
 - (a) Store any Information in electronic format on secure systems that comply with the requirements set out in the UBC Information Security Standards.
 - (b) Protect any Information in electronic format with passwords and encryption in accordance with University standards;
 - (c) Transmit any Information in electronic format using a University-provided email account or other secure network connection (I will not use third party email and storage services such as Gmail, Hotmail, Dropbox and Google Docs for this purpose);
 - (d) Protect any Information in hardcopy format using reasonable physical security precautions;
 - (e) Retain the Information only as long as it is required for authorized purposes; and
 - (f) Securely delete or destroy the Information when I no longer require it for authorized purposes.
4. I understand that I am responsible for protecting the password(s) I use to access the LMS. I will:
 - (a) Comply with the University's password complexity requirements;
 - (b) Refrain from sharing my password(s) with anyone else; and
 - (c) Comply with the [Campus-Wide Login \(CWL\) Terms of Use](#).
5. I understand that my authority to access the Information is limited to the Faculty and Departments listed in the Systems Access Level section of this form. If I become aware that my level of access is inconsistent with this authority, I will:
 - (a) Immediately report this to lt.hub@ubc.ca; and
 - (b) Avoid accessing Information that I am not authorized to access.
6. If I am accessing the Information for a research purpose, I certify that I have Behavioural Ethics Board (BREB) approval for this research. I understand that BREB approval does not automatically constitute authority to access the Information, and that I am still subject to all of the terms of this Confidentiality Agreement, UBC Policy 89, as well as all UBC Policies and Procedures related to privacy and security of the Information.



- 7. I have read and will comply with the following documents:
 - (a) Policy 104, Accessible Use and Security of UBC Electronic Information Systems;
 - (b) UBC's Campus-wide login (CWL) account terms of use; and
 - (c) UBC's Information Security Standards

I have read and understand the above conditions and agree to abide by them.

Agreement

Name: _____

Signature: _____

Date: _____

Approval

Department Head/Program Director

Name: _____

Title: _____

Signature: _____

Date: _____

Faculty Dean/Director

Name: _____

Title: _____

Signature: _____

Date: _____