iTServices

REQUEST FORM FOR BANNER LOGINS/FORMS/REPORTS

UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY

NAME:

DEPARTMENT:

POSITION:

EXTENSION:

BANNER ID #:

NEW HIRE – No previous Banner Username. Please list below the Banner functions required (i.e. Registration, Budget Access

☐ New Staff Position Start Date:

☐ Contract Position Start Date:

All date fields: DD/MM/YYYY

Finish Date:

Banner Access Required: Include additional access requests for Impromptu and Advisor in My Campus

NEW HIRE REPLACEMENT – New staff member requires access to previous employee's Banner Username to all forms and reports assigned to that Username.

Previous staff Banner Username is: Start Date:

TERMINATION OF EMPLOYMENT – Please invalidate Banner Password

☐ Leaving/Retiring Last Day: Banner Username:

CURRENT STAFF – Request for additional access Banner Username:

Form: ☐ Query ☐ Modify **Report:**

Form: ☐ Query ☐ Modify **Report:**

Form: ☐ Query ☐ Modify **Report:**

I agree to abide by the security and confidentiality guidelines as established by UOIT. I agree to supervise this person in the use of Banner Security Classes.

Manager Signature: **Date:**

Manager Printed Name:

I agree to abide by the security and confidentiality guidelines as established by UOIT.

Employee Signature: **Date:**

Employee Printed Name:

Approval: **Date:**

Designated Data Steward

December, 2011

This information is being collected for the purpose of Banner Data Access. The information provided is confidential and subject to UOIT policies concerning freedom of information and protection of privacy as well as any applicable laws. If you have questions concerning the collection of this information, please contact ITS, Administrative Services at 905.721.3111 ext. 2228.

iTServices

USE OF CAMPUS DATA
STATEMENT OF RESPONSIBILITY AND RULES OF CONDUCT

UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY

All University employees and authorized systems users are responsible for the security and confidentiality of University data, records, and reports. Individuals who have access to confidential data are responsible for maintaining the security and confidentiality of such data as a condition of their employment. The unauthorized use of, or access to confidential data is strictly prohibited.

The system access rules of conduct and user responsibilities include but are not limited to:

1. System users shall not personally benefit or allow others to benefit by knowledge of any special information gained by virtue of their work assignments or system access privileges.

2. System users shall not exhibit or divulge the contents of any confidential record or report to any person, except in the execution of assigned duties and responsibilities.

3. System users shall not knowingly include or cause to be included in any record or report a false, inaccurate, or misleading entry.

4. System users shall not knowingly expunge or cause to be expunged a data entry from any record or report, except as a normal part of their duties. Due caution will be exercised in the disposal of documents and reports containing sensitive information.

5. System users shall not publish or cause to be published any university reports, records or other information, which contains confidential information for unauthorized distribution.

6. System users shall comply with information security procedures and rules of conduct as promulgated by the University.

7. System users shall not share passwords with office workers or anyone else, have it written down, stored, transmitted on computer systems, or imbedded within automatic log in procedures, and shall take all reasonable steps to ensure access to such information is not accidentally acquired through such passwords either on campus or through remote access services.

8. No person shall aid, abet or act in concert with another to violate any part of these rules.

In addition to the above responsibilities the users of SCT applications (the software used to access campus data) must comply with the conditions of the license agreement to not sell, give away, or circulate part or all of the SCT system that may reside on the user's computer or other campus computers to anyone else. The SCT applications are the property of SCT and that must be treated as confidential information. Should you have any questions regarding the conditions for use of the system, please contact the Director, IT Services, and Administrative Systems.

I have **read** and fully **understand** the Statement of User Responsibility and Rules of Conduct printed on this form and shall comply with such statement and rules. I understand that violation of such may result in loss of information access privileges, reprimand, suspension, or dismissal in such manner as is consistent with university procedures and to prosecution under federal and provincial computer and information security laws.

User Name (Please Print):

User Signature:

Date (DD/MM/YY):

Email Form | Reset Form | Print Form