|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | THE UNIVERSITY OF BRITISH COLUMBIA **HRMS ACCESS REQUEST FORM**  (Access to Legacy HR System: Data as of October 28, 2020) | | | | | | | CWL ID (MANDATORY) | | NEW ACCESS:  DELETE ACCESS:  CHANGE ACCESS: |  | |
|  |  | | | | | | |  | |  |  | |
| APPLICANT INFORMATION (for whom HRMS access is required) | | | | | | | | | | | | |
| NAME | | | DEPARTMENT NAME | | | POSITION/TITLE | | | | UBC EMPLOYEE ID | | |
|  | | |  | | |  | | | |  | | |
| EMAIL ADDRESS | | | INDICATE HRMS DEPTIDs REQUIRED FOR ACCESS (REFER TO DEPTID LINK BELOW) \* | | | APPT START DT (YYYY-MM-DD) | | | APPT END DT (YYYY-MM-DD) | | | |
|  | | |  | | |  | | |  | | | |
| SIGNATURE (I ACKNOWLEDGE THE TERMS AND CONDITIONS FOR HRMS ACCESS – Page 2 of this Form) | | | | | | DATE (YYYY-MM-DD) | | | PHONE NUMBER | | | |
|  | | | | | |  | | |  | | | |
| FACULTY/DEPARTMENT AUTHORIZATION (signing authority for department(s) access is being granted to) | | | | | | | | | | | | |
| NAME | | | DEPARTMENT \* | | | POSITION/TITLE | | | | | | |
|  | | |  | | |  | | | | | | |
| SIGNATURE (I ACKNOWLEDGE THE TERMS AND CONDITIONS FOR HRMS ACCESS – Page 2 of this Form) | | | | | | DATE (YYYY-MM-DD) | | | PHONE NUMBER | | | |
|  | | | | | |  | | |  | | | |
| ACCESS REQUIREMENTS – Complete this section for new access or changes to existing access | | | | | | | | | | | | |
| ACCESS REQUIREMNTS - Check all that apply | | | CHK | ADDITIONAL INSTRUCTIONS OR COMMENTS | | | | | | | |
| Employee Data (includes access to Query Reports) | | |  |  | | | | | | | |
| Position Management | | |  |  | | | | | | | |
| eRecruit | | |  |  | | | | | | | |
| ePAF | | |  |  | | | | | | | |
| Other  (Provide details in Additional Instructions or  Comments area) | | |  |  | | | | | | | |
| HRMS SECURITY ADMINISTRATOR USE ONLY | | | | | | | | | | | | |
| HRMS OPERATOR ID | | PRIMARY PERMISSION  HCPPUBCPRIMEP | | | ROW SECURITY  HCDPUBC | | ROLE OR TEMPLATE | | | | | |
| COMMENTS | | | | | | | | | | | | |

\*FOR 4-LETTER HRMS code, press Ctrl-click:   
[HRMS DeptID LookUp](http://www.hr.ubc.ca/field_values/lookups/) Email this form to HRMS.Security@ubc.ca [Help](http://www.hr.ubc.ca/forms/hrms_access_request_help.html)

## TERMS AND CONDITIONS FOR HRMS ACCESS

Human Resources records available from the Human Resources Management System (HRMS) are confidential and the property of the University of British Columbia. Unauthorized access, use or disclosure of these records is prohibited under UBC’s Policy #104 (Acceptable Use and Security of UBC Electronic Information and Systems) and UBC’s Information Security Standards, and may also violate the BC *Freedom of Information and Protection of Privacy Act*.

Users of the HRMS system must take reasonable steps to protect relevant 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 HRMS system access privileges granted through their authority, by ensuring that:

1. the level of access is sufficient but not excessive;
2. users granted access privileges are aware of these terms and conditions and accept individual accountability and responsibility for use or abuse of these privileges; and
3. users’ access privileges are deleted by completing this form in a timely manner when necessary (e.g. when the user has left UBC or your department).

HRMS users are responsible for the prudent and secure use of the system in compliance with good business practice, UBC’s Policy #104 and UBC’s Information Security Standards. HRMS users are individually accountable for all system access using their access credentials (user identification code and secret password). HRMS user responsibilities include, but are not limited to:

1. keeping their access credentials confidential;
2. ensuring that their access credentials are not used by unauthorized persons to access the system;
3. ensuring that workstations are not left unattended while connected to the system; and
4. ensuring that sensitive information displayed on their workstations or hard-copy reports is not visible to unauthorized persons.

Compliance with these terms and conditions UBC’s Policy #104 and the Information Security Standards are basic terms of continued administrative system access privileges. Failure to comply with these terms and conditions could result in removal of access privileges as well as disciplinary action up to termination of employment.