a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD U10
Accessing Electronic Accounts of Other Users

1. Introduction

1.1 This document defines standards that Users (typically supervisors and investigators) must comply with to gain access to electronic accounts of other Users on UBC Systems, such as UBC email accounts, UBC file sharing, collaboration and messaging accounts, Home Drive, voicemail accounts, internet usage records and telephone logs.

1.2 This standard does not apply to electronic accounts that are not owned by individual Users, such as building access logs or shared email accounts.

1.3 This standard does not apply to system administrators or other technical personnel who, in the course of carrying out their duties, require access for technical purposes, such as installation, maintenance, repair, troubleshooting or upgrading.

1.4 The purpose of this standard is to protect the Personal Information of individual account holders while continuing to allow access to information required for University purposes.

1.5 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Access with Consent

2.1 Policy SC14 authorizes reasonable personal use of UBC Systems. For privacy reasons, it is preferable to get the consent of Users before accessing electronic accounts and records.

2.2 Consent must be in writing, but does not need to be signed (an email is acceptable). The following language is recommended for a consent statement:

> I, [NAME], authorize UBC to access [ACCOUNTS/RECORDS] for the following purpose: [PURPOSE]. This authorization is effective until [DATE].

2.3 If the consent of the User has been secured, authorization of the Administrative Head of Unit or the Office of the University Counsel is not required to access the account or records in question.

3. Access without Consent

3.1 It is occasionally necessary to gain access to an electronic account or record without the User's consent. To ensure that the University's Business requirements are balanced against the User's privacy interests, access without consent requires the authorization of the Administrative Head of Unit and the Office of the University Counsel. This authorization will depend on the type of information intended to be accessed and how the information will be used after it has been accessed.

4. Criteria for Access to UBC Electronic Information without Consent

4.1 If UBC Electronic Information only needs to be viewed, then the Administrative Head of Unit and the Office of the University Counsel will authorize access the electronic accounts/records provided that:

4.1.1 there is a pressing reason to view this information for University Business purposes; and

4.1.2 consent of the User cannot be secured despite making reasonable attempts to do so, e.g. the User is incapacitated, has gone on vacation without leaving contact information, or has been terminated and is unwilling or unavailable to provide consent.

Example

An employee has been incapacitated in a motor vehicle accident. Her supervisor needs to access the employee's work email account to check for any time-sensitive work-related messages, but the employee is unable to consent to this access. Under these circumstances, access would normally be authorized. However, the supervisor should not read the employee's personal messages.

4.2 When accessing accounts or records to view UBC Electronic Information, reasonable efforts must be made to avoid viewing the User's Personal Use Records. If Personal Use Records have been inadvertently viewed, then these records must not be copied, altered, deleted, used or disclosed unless they provide evidence of a violation of law, in which case the matter must be referred to the Office of the University Counsel, which will determine the appropriate action.

4.3 In addition to Personal Use Records, accounts may also contain other sensitive information, such as teaching materials or research information. The confidentiality of this information must be respected as its unauthorized use and disclosure may harm the interests of the User and the University as a whole.

5. Criteria for Access to Personal Use Records without Consent

5.1 If Personal Use Records need to be viewed, then the Administrative Head of Unit and the Office of the University Counsel will only authorize access to electronic accounts/records if the University is legally required to do so, or if securing consent would compromise:

5.1.1 the health or safety of an individual or a group of people,

5.1.2 the availability or accuracy of the information; or

5.1.3 an investigation or a proceeding related to a breach of law or policy or the employment of the User.

6. Procedure for Access

6.1 To access accounts and records, the Request to Access Electronic Accounts of Other Users form must be completed and submitted to the administrator who controls access to the account. If the User's consent is not obtained, the Administrative Head of Unit and the Office of the University Counsel must be requested to sign the access form to authorize access. The administrator will grant access to the account/records only for the period of time specified in the access form.

7. Related Documents and Resources

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

Request to Access Electronic Accounts of Other Users form