



Request For Reusable or Generic Administrative Logonid

For authentication and audit purposes, UTS must be able to identify the individual who is responsible for all computing activity performed while logged in under any given logonid. In general, this means that one and only one individual is associated with a single logonid.

Requests for a logonid that can be reused by more than one individual may arise from departments where a job function is filled by one or more temporary staff, often on a recurring basis, but not necessarily by the same individual. In a few, rare situations a generic logonid may be required for permanent employees to differentiate computing activity that is limited to a very specific application.

Where a single temporary employee is filling a job for more than one month, it is preferable to create a new unique logonid with appropriate access rules for that individual. An expiration date can be set for the logonid so that it cannot be used beyond the duration of the appointment without explicit action.

In making this request for a reusable logonid for use within my department, I agree that:

I accept responsibility for all computing activity performed under this logonid;

I will maintain a log showing the range of dates and names of all individuals who use the logonid. This log will be made available upon request;

I will control the use of the logonid by changing the password when the temporary staff assignment is complete (Note. To disable the logonid when it is not needed for an extended period of time, contact the mainframe security group via email datasec@mcmaster.ca).

(Please print. Return completed form to Data Security Requests, UTS, GH 302)

Name: _____ McMaster ID: _____

Department: _____ Campus Address: _____

Job Title: _____ Campus Phone: _____

E-mail: _____

Signed: _____ Date: _____

Supervisor's Approval: _____ Date: _____

Logonid Assigned: _____

