Policy for the Provision of Privileged Access (*sudo*)

Overview

Occasionally it is desirable for a specific member of the department to be able to issue a particular command on a named system with privileged access, *e.g.* to restart or update a daemon, especially so on a research development server. For Linux/Unix systems one way to provide such privileged access is via the *sudo* command.

Purpose

The purpose of this policy is to clearly define how authorised members of the department may be provided with access to privileged commands on specific systems.

Scope

The scope of this policy is to define the policy by which authorised personnel may be provided with access to elevated privileges to perform specific tasks. This policy pertains to all computer systems, networks, hardware, software and firmware owned and/or operated by the department.

Policy

When the computing manager receives a request for privileged access from an authorised user to perform a specific task on a given computer, consideration should be given to the benefits and risks involved, the role the computer provides, options and solutions available, along with the experience and computing knowledge of the user.

Approval is entirely at the discretion of the computing manager on the understanding that privileges maybe withdrawn at any point in the future without prior notice. All privileges will be reviewed from time-to-time to ensure they remain appropriate for the work being performed.

When a research server is involved, the computing manager will consult with the research group leader to obtain their approval.

If the user is a student and the computing manager intends to approve the request, the computing committee chair should be informed of the full details of the request, and their approval also obtained.

Enforcement

Where this policy is found not to have been followed, corrective action should be taken to promptly achieve compliance and the computing manager notified. The computing manager may notify the chair of the computing committee, especially where further disciplinary and/or other action may be considered appropriate.

Definitions

- Authorised user – A user authorised by the department to be using the computing facilities provided.
- Privileged access – authorised users usually have limited access to interact only with their own processes on the computer. However by granting limited privileged access they can also be given specific rights to restart or reconfigure processes running as another user or daemon.
- sudo – the *sudo* command on Linux/Unix systems allows permitted users to execute specific commands with privileged access as the superuser or another user, as specified in the configuration file.

Revision History

- November 2011 – Discussion at computing committee meeting
- January 2012 – First policy draft
- February 2012 – Approved by CC