Procedure: Information technology local administrator privileges

Purpose
The purpose of this procedure is to:

- describe how ANU manages the provision of local administrator privileges on Information Technology Services (ITS) supported workstations, laptops and mobile devices; and
- define the standards, expectations and responsibilities of ANU employees who are granted these privileges.

Definitions
Definitions of additional terms used in this document are provided in the overarching Information technology security policy.

Local administrator privileges: the provision of unrestricted access to the operating system. This allows the user to install any hardware or software, edit the registry, manage the default access accounts and change file level permissions.

Procedure
1. This document applies to ITS supported workstations, laptops and mobile devices and encompasses all devices in areas of the University where information technology (IT) services are delivered centrally by ITS.
2. ITS supported devices are managed under a controlled Standard Operating Environment (SOE). The SOE has restrictions in place to prevent users making system changes or installing software on their device with the aim of ensuring the highest level of stability and security.
3. Users who require access to their device beyond that granted under the SOE may apply for local administrator privileges.
4. Users may submit requests for local administrator privileges to the ANU Service Desk using the Request for administrator privileges form. The requests are authorised by a School Director, School Manager, Associate Director or equivalent. The user must include an explanation for the request.
5. Applications are assessed by the Team Lead, Standard Operating Environment.

6. A user who does not have administrator privileges and who requires system changes or software installed will require the assistance of the ANU Service Desk. A Service Desk Officer performs these tasks via remote access.

User responsibilities

7. Any software or applications downloaded or installed by the user are for University purposes only.

8. Software and applications are downloaded from official vendor sites. Users adhere to the relevant license agreement.

9. Users ensure that any software they have installed is kept patched to the current version.

10. Users do not download or install:
   a. illegal or unlicensed applications and software;
   b. software which adversely impacts the operation of the network or any other system. Users employ caution when downloading and installing software so as to also avoid downloading malicious software.

11. In the event a device becomes compromised, the user:
   a. informs the ITS Cyber and Digital Security Team by emailing it.security@anu.edu.au;
   b. re-installs all self-installed software if re-imaging is required; and
   c. backs up any data stored on their device prior to re-imaging, if required.

12. Sophos anti-virus updates are pushed to devices by group policy. Users must not:
   a. alter, upgrade or remove any software installed by ITS;
   b. install any other anti-virus software that might interfere with Sophos;
   c. override, disable or remove the Universities anti-virus solution from their device; and
   d. disable any security mechanisms put in place by IT Services, including antivirus protection, firewalls, software/patching deployment mechanisms (e.g. System Center Configuration Manager) or other services.

13. All ITS workstations, including laptops and Surface Pros (excluding Macs) are configured with LogMeIn Remote Support Software. This software allows authorised ITS support staff to remotely control the workstation if necessary to perform troubleshooting, and is not altered, removed or uninstalled.
The purpose of this procedure is to: describe how ANU manages the provision of local administrator privileges on Information Technology Services (ITS) supported workstations, laptops and mobile devices; and define the standards, expectations and responsibilities of ANU employees who are granted these privileges.
Please ensure you have the latest version of this document from the Policy Library website before referencing this.