Responsibilities of users with local administrator rights

Date: 22nd July 2016
Version: 1.3

Background

IT Services (Desktop Services Team) provides a standard computer build to the staff of the Bodleian Libraries and UAS. The use of a standard computer build ensures that software and services work in a consistent fashion. The standard computer build is locked-down, i.e. users do not have local administrator rights and so cannot install software or make configuration changes to computers. Computers are locked down for a number of reasons:

- Systems are more secure if users are unable to change security settings or load software with unknown security properties;
- Software license compliance is easier to achieve when there is control over which software can be installed;
- Users gain from more timely support because changes are made in a controlled fashion and the support staff do not need to spend time familiarising themselves with a new system each time a support call is raised;
- It is easier to test and deploy new software on configurations that are stable;
- There is a reduction in the total cost of ownership (TCO) of computers when they are locked down[1].

However it is recognised that certain types of user need to have local administrator rights in order to efficiently carry out their daily work. Examples of roles compatible with local administrator rights include software developers, staff who routinely evaluate new software and laptop users. There are risks associated with local administrator rights including security compromises[2], breaking existing systems, license non-compliance and additional support burden. For this reason users granted local administrator rights have certain responsibilities. This document describes the responsibilities of users that have been given local administrator rights.

Local Administrator Account

Users that require local administrator rights should complete an IT Services Service Request form. They should give justification for their request and their request should be authorised by their head of department. Users will usually only be granted local administrator rights if their role requires significant software development, regular evaluation of new software or they are a laptop user.

[1] Gartner have estimated 18% reduction in direct costs and 54% reduction in indirect costs with lockdown (Gartner, 28 September 2005, ID Number G00120859 ‘Consider User profiles in Implementing Desktop Lockdowns’).

[2] Compromises can result in incidents such as loss of data, breaches of confidentiality and network flooding, bringing all internal network traffic to a halt. Compromised computers may also be used to initiate attempts to compromise other computers outside the University, or to launch floods of ‘spam’ email.

If a request for administrator rights is approved the user will be given an additional user account with local administrator rights privileges. This local administrator user account will be limited to a single machine and will not work on other computers. They should use their normal user account for most work and only use the local administrator account when they need to install new software or make configuration changes. This approach is required because there are security risks associated with using an administrator account continuously as viruses and malware can do much more damage when run with administrator privileges.

User Responsibilities

- Limit use of the local administrator account for installing software and making configuration changes. The normal user account should be used for the majority of daily computer use.
- Not to tamper with computer security settings, including firewall, anti-virus and lock-down settings.
- Not to alter or remove computer management agents and services, e.g. Altiris agents.
- Not to add additional peripheral devices, that would require Administrator access (e.g. printer, scanner, wireless network devices, etc.) without prior consultation with Desktop Services Team.
- To avoid installing software with known security risks without applying and documenting mitigating measures.
- To be responsible for all software and configuration changes that they have applied.
- To create and document a support plan (potentially involving 3rd party support) for any software that they have installed, if support is required, and to gain their line-manager's sign-off on that plan. If the plan calls for IT Services' resources, it will require sign-off from the Desktop Services Manager.
- To monitor security alerts for all software that they have installed and ensure that security patches and product updates are applied in a timely fashion.
- To satisfy the license conditions of software that they install and ensure that they purchase any necessary licenses.
- To provide Desktop Services Team with copies of licenses purchased for any software that they have installed.
- Accept that if any software installation or configuration change breaks the existing computer build then Desktop Services Team will provide no more than 30 minutes troubleshooting assistance before re-imaging the computer.
- To use the IT Service HFS service to back up their computer and to restore their customisations in the event that their computer needs to be re-imaged.
- Recognise that tools and services developed on non-standard (i.e. customised) computers may not work as expected on standard computer builds.
- Commit to keep Desktop Services Team informed about development of new tools and services and to give reasonable notice of intention to roll out to a wider audience. Then to collaborate on development of effective deployment and management processes, prior to handover.
- To use the IT Services' Service Desk (help@it.ox.ac.uk, x12345) when requesting information, support or help.

- To accept that provision of local administrator rights will be regularly reviewed.

Desktop Services Team Responsibilities

- To provide a standard computer build and standard computer services as per those provided for the CONNECT Service
- Desktop Services Team will provide no more than 30 minutes troubleshooting assistance before re-imaging any computer that has been customised by users with local administrator rights.
- Desktop Services Team will restore computers to the standard computer build in the event that 30 minutes troubleshooting does not resolve reported issues.
- Desktop Services Team will provide assistance with setting up the backup of user's computers using the IT Services HFS service.
- Desktop Services Team will maintain the security of computers and remove software or reimage machines if a security compromise is identified or suspected.
- Desktop Services Team will respond to support requests in a timely fashion.

Acceptance

Name:

Department:

Signature:

Date:

This form is issued by Desktop Services and MUST NOT be copied for re-use