University of East Anglia

ISC11D041

Title:	**PC AND LAPTOP ADMIN RIGHTS**
Author:	Steve Jackman (ISD)
Date:	November 2011
Circulation:	ISSC - 3 February 2012
Agenda:	ISC11A002
Version:	v2
Status:	Open

Issue

To describe the procedures for the provision of administrative rights to PCs and laptops.

Recommendation

Recipients are invited:

- To receive the report.

Resource Implications

No change to service is required and therefore there is no impact on resources.

Equality and Diversity

New services will be subject to Equality Impact Assessments as they are implemented.

Timing of decisions

No decisions are required.

Further Information

- Steve Jackman (ISD), x7615, s.jackman@uea.ac.uk

Background

The committee considered this issue in its meeting on 10th November 2011, and asked for more detailed guidelines on administrative rights for locally administered laptops. This paper is in response to that request.

Discussion

Title: **PC AND LAPTOP ADMIN RIGHTS**
Author: Steve Jackman
Date: November 2011
Version: v2

Background

PCs and laptops are used extensively by staff and students, both on and off campus. Network access is provided by wired connections on campus for access to resources behind the firewall – i.e. day-to-day activities such as file store access, printing and access to line of business systems. Wireless access via wi-fi (e.g. Eduroam) is provided for access to resources outside of the firewall including web-based services and the Internet. PCs and laptops may also be connected to other networks while off-site, e.g. domestic broadband connections or access via another institution.

Staff PCs and laptops with full network access will have been configured by UEA IT staff to ensure their security and compliance with corporate policies. Regular contact with the wired network ensures that licensing provision is maintained as well as updates to anti-virus (AV) software and operating system (OS) patches.

From time to time laptops, and occasionally PCs, may be removed from campus for extended periods in the normal course of work, which can affect their security if AV and OS updates have not been applied. Machines with local administrator rights available to the user are particularly vulnerable to being compromised, which increases with the elapsed time since the last AV update. In particular:

- Access to compromised web sites may install viruses, malware or spyware programs (automatically disabling any anti-virus tools installed).
- Documents may install viruses, malware or spyware programs.
- Emails may install viruses, malware or spyware programs.
- Malicious programs may publish or destroy data (including documents held on your central file store and other windows file shares).
- Malicious programs will be able to spread to other machines and devices that have appropriate rights for them to install themselves on (such as another PC, laptop, mobile phone or iPad).

Administrator rights are often needed by users:

- To enable connections to external networks or printers, e.g. to domestic broadband wi-fi, where the operating system is older than Windows 7
- To enable the installation of software or updates to existing packages

PC and Laptop Treatment

1. As a matter of course, UEA-owned PCs and laptops will be configured to run the latest version of the relevant operating system with administrator rights disabled[1] for users, in order to minimise the risks associated with the threat of compromise. In certain circumstances an exception may be applied to this as set out below.

2. PCs and laptops built and configured by UEA IT staff are normally considered as being 'on the *wired* network' – i.e. they may connect to the *wired* network with full access.

3. Where a PC or laptop is taken away from the *wired* network for a period of more than one month, the risks are such that the device must then be considered 'off the *wired* network'. It can still connect to the *wireless* network, but must be checked and if necessary re-imaged by UEA IT staff before it can be connected to the *wired* network, to ensure that it is virus free and up-to-date.

4. Some staff laptops as well as student and visitor laptops (and other devices such as smartphones) may permanently be treated as 'off network', and do not therefore need to be built or (re)configured by UEA IT staff. In such circumstances staff should be aware of potential licensing issues – contact IT support for advice.

Requesting Local Administrator Rights

Anyone can request local administrator rights to be granted on their PC or laptop. A member of IT support staff will assess and advise if it is possible to achieve the user's aims via another route, e.g. by installing software for them. In some cases the installation of a second 'sand box' environment may be an appropriate solution. If it is adjudged that local administrator rights are appropriate and necessary then this will be enabled and a record made in the IT security risk log. This log will be reviewed on a regular basis.

Users should follow the process set out below:

***Step 1*:** Contact the IT Helpdesk

Contact the IT Helpdesk (Email helpdesk@uea.ac.uk or Telephone ext. 2345) with details of the requirement, e.g. software that needs to be installed including proposed licensing arrangement (if appropriate).

Step 2: Visit from IT support technician

An IT support technician will then visit the user to assess the requirements and provide a solution to address the user's needs. The solution would be one of the following in order of preference:

1. *The need to install and test software*: A virtual desktop environment would be created with network connectivity and local administrator rights

[1] The removal of administrator rights by default was agreed at ISSC in June 2011

2. *An application that requires administrator rights to run:* The technician would consider the use of various Windows tools to enable the application to run as administrator (Applocker, Run As..., group policy, etc.)

3. *The need to install printers:* The user would be added to the print operators group

4. *The need to change network configuration:* The user would be added to the network operators group

5. *The user will be working in the field for a prolonged period and needs are not currently known:* The user would be given local administrator rights to the machine, it would be logged in the security risk log and the machine would be re-imaged before reconnection to the UEA wired network.

6. *The requirements cannot be met by any of the solutions above:* local administrator rights will be granted, it would be logged in the security risk log and the requirements would be reviewed after 12 months.

Step 3**:** Record exception

If the IT support technician is required to apply administrator rights to meet the user's needs, this will be recorded as an exception.

The IT support technician will need to record who has been given local administrator rights, the reason it is needed and for how long local administrator rights will need to be applied. Anyone who is given local administrator rights will be reviewed on an annual basis to see if these are still required.

Step 4**:** Applying local administrator rights

The IT support technicians apply local administrator rights for the user on their PC (can be applied remotely). The user will then need to connect the PC to the UEA wired network to allow it to pick-up the revised policies giving the user local administrator rights.

Note: Requests to have local administrator rights on a laptop that is to be taken away from UEA must be made prior to their trip. When rights have been applied users should test that they are able to install and run the software needed.