University of East Anglia

ISC11D008

Title:	**Admin rights on desktop PCS**
Author:	Jonathan Colam-French and Paul Hooper
Date:	2/11/11
Circulation:	ISSC – 10 November 2011
Agenda:	ISC11A001
Version:	Final
Status:	Open

Issue

Measures to improve the security of UEA ICT infrastructure.

Recommendation

ISSC is asked to consider the comments in the IT position paper provided by the Head of School for Economics (appendix 1)

ISSC is asked to endorse the proposed approach to Admin rights outlined in the paper.

Resource Implications

The recommended approach does not rule out the allocation of local administrative rights but does introduce a process for ensuring that these are monitored and applied sparingly, this will require some investment of time by the technicians but is not perceived as requiring any additional resources.

Risk Implications

One of the recommendations from the independent security audit was to remove all local admin rights, the IT position paper from the School of Economics makes a compelling argument for pragmatism which this recommendation recognises. Local administrative rights do increase the potential risk of IT intrusion, but this needs to be balanced against the University requirement to operate a highly diverse ICT infrastructure and manage down the costs of this provision.

Equality and Diversity

It is not perceived that this proposal will have an adverse impact on specific groups with protected characteristics.

Timing of decisions
Not applicable

Further Information
Paul Hooper (ISD)

Background
See risk implications section.

Discussion #

$ ¸æ Ł1 ⌗5 ŁÆª –1⌗1 # ˇ 1Œ–Ł ø⌗3 & 1#

Following a hacking attack on servers in the Climatic Research Unit (CRU), ISD was asked to undertake a review of the security of the UEA Network. ISD engaged with an external security company to aid them in the discovery and make recommendations for change on security issues. The use and prevalence of local administrator accounts was identified as one of a number of risks to the security of the IT network at UEA. ISD were subsequently asked by the Executive Team to put together proposals for resolving the issues and gaps in security that had been identified. The proposed changes had a requirement of funding that could not be met in the current year. ISD are taking a pragmatic approach, where possible, in resolving the issues found within the funding available.

Risks associated with use of Admin Rights

The use of Admin Rights on a PC increases the risk of the computer being compromised and of improper configuration.

- Compromised web sites may install viruses, malware or spyware programs (automatically disabling any anti-virus, malware or spyware detection 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 filestore 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 your laptop, mobile phone or iPad).

Process for Requesting Admin Rights

The use of local administrator accounts was discussed at the last meeting of ISSC (June 2011) and it was agreed that these need to be phased out which is happening as part of the roll out of Windows 7. We recognise that staff occasionally need the flexibility to install software and anyone can request for a member of IT support staff to assess the software and provide appropriate rights for the software to be installed and run via the IT Helpdesk. If IT support is unable to provide a solution for installation and recommend provision of Admin Rights then IT Support will record who is being given admin rights and the reasons for this. Admin rights will then be applied and reviewed on a regular basis.

Step 1: Contact the IT Helpdesk

Contact the IT Helpdesk (Email staff.help@uea.ac.uk or Telephone ext. 2345) with details of the software that needs to be installed and licensing arrangement (if appropriate).

Step 2: Visit from IT Support Technician

The IT Helpdesk will assign the help call to an IT support technician, who will then visit you to assess your requirements and provide a solution to address your 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 Administrator rights
2. **An application that requires Administrator rights to run:** The technician would use various Windows tools to enable the application to run as Administrator (Applocker, runas, 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 Administrator rights to the machine, it would be logged in the security risk log and the machine would be wiped and re-imaged before reconnection to the UEA Network.
6. **The requirements cannot be met by any of the solutions above**: 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 Admin 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 Admin Rights, the reason it is needed and for how long Admin Rights will need to be applied. Anyone who is given Admin Rights will be reviewed on an annual basis to see if these are still required.

Step 4: Applying Admin Rights

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

Note: Requests to have admin 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.