Elevated User Rights (EUR) on IT Equipment at the University of Bristol

Notes
This policy was approved by the Information Security, Identity and Access Management Board.

Text was updated in June 2013 to clarify adjudication route for EUR requests.

Purpose
This document provides a framework for the management of Elevated User Rights (**EUR**) – commonly referred to as 'admin rights' - on desktop systems, irrespective of underlying Operating System, at the University of Bristol, from January 2012 until it is superseded.

The application form for EUR can be found at www.bristol.ac.uk/it-services/eur

Scope
The scope of this policy is to cover those machines which are commonly described as **desktop** machines or:

- PCs, Macs or Workstations
- Laptops, Notebooks, Mac Laptops or Netbooks

These machines will be University owned and connected – permanently or temporarily – to any of the University's routed networks (docking, wired or wireless). Such machines may be on site or at home.

This policy does not cover non-University owned equipment.

Computers commonly referred to as 'Servers' are not explicitly covered by this agreement as usage is generally more restricted and controlled. However, the principles in this document apply to servers and control of EUR should be discussed with IT Services.

IT hardware which is embedded in experimental, monitoring, control systems or medical equipment is unlikely to be covered by this policy but may need to be discussed with IT Service if a PC has a dual purpose e.g. controlling equipment and being used as a desktop.

Context
This policy supports the University's IT strategy to deliver efficient, secure and cost-effective IT solutions, while supporting University colleagues in necessary creativity and variety in approaches to teaching, research and enterprise.

The controlled management of the EUR is vital to the business of the university to ensure:

- staff have a secure and reliable desktop experience
- research, personal and corporate data is protected from corruption, misuse or breach of law
- support time is minimised by reducing variable or unknown configurations
- access to the University network is limited to those with the correct authorisations
- software deployed is correctly licensed
- global updates can be applied quickly and remotely
- restore times are faster in the event of a machine failure

In the large majority of cases IT Services expect to retain full control of the EUR e.g. where machines are in public or student facing areas or all applications on a desktop are centrally managed. Running

computers with EUR always increases risk from malicious software or cyber attack or machine corruption. Vital data can be lost and/or time is lost in restoring service.

General Principles for granting EUR

IT Services recognises that instances arise where there is the need for staff to have EUR in order to do their University work. All instances need to be reviewed by IT Services on a case-by-case basis and, if approved, the implementation of EUR will also vary according to need and/or the device being used.

Because running with EUR always adds risk of data loss or computer virus or machine malfunction, IT Service will seek to keep numbers running with EUR to a minimum and therefore not all requests will necessarily be met.

Terms and conditions of use need to be read and acknowledged before EUR can be granted.

In the event of a machine malfunction IT staff will do their best to restore service as quickly as possible. However, any machine administered via EUR may have changes made that IT staff know nothing about. Because of this we can only offer a guarantee of restoring the latest version of the standard PC deployment. Staff are encouraged to store data on central file stores and not the hard disks of their PC or laptop.

EUR will be withdrawn if a particular threat is identified or, for example, machine hardware is repeatedly corrupted. Appropriate notification will be given to staff depending on the threat posed to data security.

Any software installed must be appropriately licensed.

IT Services will seek confirmation from Heads of School or equivalent in Professional Services if a) they have asked to confirm requests for EUR submitted by their staff or b) in the situation where IT Services feel an EUR request is not warranted but the requestor wants the matter referred. In most cases, Head of School (or equivalent) authorisation should be sufficient to get the EUR request approved. If further adjudication is required it should be referred to the Director of IT Services.

The names and machines of staff running with EUR may be recorded and circulated within IT Services or subsets of names provided to relevant line managers.

Generally EUR, if granted, will be for one staff member and one machine. EUR for one user over multiple machines will only be granted in truly exceptional circumstance due to security risk and privacy concerns.

Responsibilities of staff: All University staff, irrespective of whether or not they have been given EUR, have the responsibility of ensuring that their use of Information and Communication Technologies conforms to legal requirements, and to the University's information security policies. These policies can be found at http://www.bris.ac.uk/infosec/policies