ISC10D028

Report Control Information

Title:	Security Manual - SM5.3 System Administrator passwords
Date:	19 January 2011
Version:	v1.2 (as approved by ISSC xxxxx)
Reference:	ICT/SECMAN/SM5.3/v1.2
Authors:	Steve Mosley
Quality Assurance:	ISSC

Revision	Date	Revision Description
V1.0	17/1/06	Final version as approved by the Information Strategy and Services Committee (ISSC) on 2nd of December 2005.
V1.1	18/5/09	Change to location of password best practice advice under SM5.3.1.
V1.2	18/1/11	Revisions as part of security policy review following investigation and recommendation by security consultants

SM5.3 System Administrator passwords

Security Control	Policies governing assignment and handling of system administrator passwords.
Objective	To ensure that system administrator passwords (including Domain Administrator and root passwords) are assigned, maintained and stored securely.
Responsibility	Information Services is responsible for ensuring that administrator passwords on systems which they manage are assigned and handled in a secure manner in accordance with these policies. All staff are responsible for ensuring that administrator passwords on computer systems which they manage are assigned and handled in a secure manner in accordance with these policies.
Incident management	Where system administrator security is discovered to have been breached, this should be reported immediately to the support staff responsible for security of the system. If it is discovered that the security controls described here have not been adhered to, the matter should be referred to senior management responsible for the system(s) involved.
Audit and accountability	System owners who have computer systems in their care, will on a regular basis review administrator password security arrangements and check that the procedures described here are being followed. In particular they will check that written records of administrator passwords and those with authorised access are accurate, are stored securely and are not available to unauthorised personnel.
Implementation	**Server administrators (including domain administrator and root accounts)** SM5.3.1 Wherever possible, support staff whose role requires administrator privileges on a server should have those privileges applied to their normal UEA IT account by including them as a member of the appropriate administrator's group within Active Directory. If their role changes and system administrator privileges are no longer required,

they should be promptly removed from the administrator's group[1]. Where actual system administrator passwords have to be disclosed to support staff, policies SM5.3.2 to SM5.3.5 should be applied.

SM5.3.2 All system administrator account passwords (including domain administrator and root accounts) should adhere to the password assignment rules as defined in the Security Manual SM5.1 ' Password assignment' and except for additional requirements as applied to administrator account passwords, follow best practice as published at http://www.uea.ac.uk/is/itregs/userguide.
Wherever possible the password should be randomly generated and should be unique to the computer/service.

SM5.3.3 System administrator passwords should be disclosed to as few staff as is practically possible in order to maintain operation of a service. Procedures should be in place to ensure that disclosure of passwords is only authorised by the manager of the system(s) and to ensure that those receiving the password acknowledge receipt and their responsibility to keep the password secure and not disclose it to others.

SM5.3.4 System administrator passwords must be changed on a regular basis, at least twice per year and whenever a member of staff who has known the password ceases to be employed by the University, or moves to a different post whose duties do not require system administrator access to the system(s) concerned.

SM5.3.5 A written record of the current system administrator password along with a list of those to whom it has been disclosed, should be stored in a safe and secure place, access to which is restricted to the manager responsible for the system(s) and a nominated deputy. All previous records of system administrator passwords should be destroyed.

Desktop local administrator accounts

SM5.3.6 Where possible, desktop local administrator accounts should be disabled. If this is not possible, they should only be enabled for the duration of the requirement.

SM5.3.7 IT support staff, whose role requires that they have local administrator access to desktop systems in their care, should have those privileges applied to their normal UEA IT account by including them as a member of the appropriate administrator's group within Active Directory. If their role changes and system administrator privileges are no longer required, they should be promptly removed from the administrator's group.

SM5.3.8 Separate administrator groups should be set up for each department following Active Directory Organisational Units (OUs) and IT support staff computers should be excluded so that they do not automatically have administrator privileges on their own computer.

SM5.3.9 Desktop local administrator account passwords should only be used where privileges as described above in 5.3.7 are insufficient to resolve a problem, and direct access via the local administrator account is essential. In such cases controls SM5.3.10 to SM5.3.16 should be applied. Procedures should be in place to ensure that the password is only distributed to authorised IT support staff and a log is maintained of

[1] When staff leave UEA their IT account is automatically deleted and hence their membership if the administrator group.

those who have access to the password.

SM5.3.10 Staff (including IT support staff) requiring local administrator privileges on their office computer will have to request this from their department’s IT support staff and give justification for this. Local administrator privileges will only be granted for a finite period of time.

SM5.3.11

SM5.3.12 The local administrator account password on a desktop system should adhere to the same password assignment rules as applied to servers and defined in SM5.3.2.

SM5.3.13 The local administrator password should only be disclosed to those IT support staff who have responsibility for supporting and maintaining the system and only when the usual administrator privileges granted to them are not sufficient to fix a problem – see SM5.3.8

SM5.3.14 Local administrator passwords should be disclosed to as few staff as is practically possible in order to maintain operation of a service. Procedures should be in place to ensure that disclosure of passwords is only authorised by the manager of the system(s) and to ensure that those receiving the password acknowledge receipt and their responsibility to keep the password secure and not disclose it to others.

SM5.3.15 Local administrator passwords must be changed on a regular basis, at least twice per year and whenever a member of staff who has known the password ceases to be employed by the University, or moves to a different post whose duties do not require system administrator access to the system(s) concerned.

SM5.3.16 A written record of the current local administrator password along with a list of those to whom it has been disclosed, should be stored in a safe and secure place, access to which is restricted to the manager responsible for the system(s) and a nominated deputy. All previous records of system administrator passwords should be destroyed.