ISC10D027

Report Control Information

Title:	Security Manual - SM5.1 Password assignment
Date:	28 January 2011
Version:	v1.1 (revised for approval by ISSC)
Reference:	ICT/SECMAN/SM5.1/v1.1
Authors:	Steve Mosley
Quality Assurance:	ISSC

Revision	Date	Revision Description
V1	12/1/06	As approved by ISSC December 2005
V1.1	19/1/11	Revisions as part of Security Review project and based on recommendations following external consultants report.

SM5.1 Password assignment

Security Control	Policies governing assignment of passwords
Objective	To ensure that all University computer systems conform to a single set of secure password rules/policies.
Responsibility	Information Services is responsible for defining University rules and policies regarding passwords. IT support staff must ensure these defined rules/policies are applied to all computer systems that they are responsible for.
Incident management	If a password on a computer system is found to be insecure and does not conform to the defined rules/policies, it should be reported immediately to the IT support staff responsible for that system.
Audit and accountability	All IT support staff will on request by Information Services confirm that all computer systems under their control are using the University's defined rules/policies for passwords. For computer systems whose authentication is against the Active Directory, the defined rules/policies will be automatically applied to both local and domain user accounts.
Implementation	SM5.1.1 All user accounts on University computer systems, irrespective of the type of computer system or account, must be assigned passwords which meet the following minimum requirements. • User account passwords must be at least eight characters in length • Administrator account passwords must be at least fifteen characters in length • Not contain all, or part of the user's account name • Contain characters from three of the following four categories: English upper case characters (A through Z) English lower case characters (a through z) Base 10 digits (0 through 9)

	Non-alphanumeric characters (e.g. !, $, #, %) SM5.1.2 Authentication mechanisms should force the user to change from their default assigned password to a new one at first login to the system. SM5.1.3 All mechanisms for assigning or changing passwords should be set to automatically apply the rules in SM5.1.1 and in addition ensure that the previous password from the password history cannot be used. SM5.1.4 Passwords must be stored on computer systems as a non-reversible cryptographic hash using the strongest hash available for the operating system. For Windows based systems a NoLMHash policy should be applied to avoid storing passwords as Lan Manager hashes, instead using the stronger NT/Unicode hash. Passwords should not be transmitted in plain text format for any purpose. Access to stored cryptographic hashes must be restricted to as few people as is possible whilst allowing normal operational and administration procedures to be undertaken. SM5.1.5 Defined procedures must be followed when communicating default passwords to computer users – see Security Procedure SP1 'Communicating passwords to users'. SM5.1.6 Additional defined policies and procedures are to be followed for the storage and handling of system administrator passwords (see Security Manual SM5.3 'System Administrator Passwords').