GISP5. Use of passwords

Date:	5 October 2017
Version:	3.0
Authors:	Raymond Scott
Quality Assurance:	Information Strategy and Services Committee (ISSC)

Version control

Revision	Date	Revision Description
1.0	8/11/12	Approved by ISSC
1.1	28/5/13	Procedure for communicating passwords reviewed
2.0	11/6/13	Approved by ISSC
2.1	5/10/17	Reviewed and updated
3.0	20/10/17	Approved by ISSC

Policy

Security Control	Access to all University computer systems is controlled by use of individual usernames and passwords.
Objective	To prevent unauthorised access to computer systems.
Policy	5.1. All access to University computer systems will be controlled by use of a unique username and password limiting access to each user of the system. 5.2. All default passwords assigned to individuals will be secure and follow defined rules. 5.3. System administrator passwords will be restricted to specific authorised personnel following defined policies and procedures. 5.4. Access to operating system commands and application system functions is to be restricted to those persons who are authorised to perform systems administration or management functions. Where appropriate, use of such commands should be logged and monitored.
Responsibility	• Individual users are responsible for keeping their password secure and not divulging it to anyone else. • If individuals change their password, they should ensure that it is secure and conforms to University approved best practice as published on the ITCS website. • Those responsible for assigning and communicating passwords to individuals must follow rules and procedures as detailed below in 'Communicating passwords to users'. • Passwords should not be disclosed to anyone other than the individual concerned.
Incident Management	• If a user's password (and hence their IT account) is found to have been compromised, it will be changed immediately by ITCS to a new secure one and the user informed.

	• Where an individual suspects that an unauthorised person is using another's password to access University computer systems, they should report the incident immediately to the IT Service Desk. • 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	All IT support staff will on request by ITCS 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. A risk assessment should be undertaken for any IT system which is not capable of supporting the password policy, this risk assessment should be reported to ISSC. 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	**All Users**
	• 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
	  • Passwords for administrator accounts and user accounts with administrative rights must be at least fifteen characters in length
	  • Not contain the user's account name
	  • Contain characters from at least three of the following four categories:
	  1. English upper case characters (A through Z)
	  2. English lower case characters (a through z)
	  3. Base 10 digits (0 through 9)
	  4. Non-alphanumeric characters (e.g. !, $, #, %)
	• Passwords should expire 365 days after the date they were last changed or created.
	• Authentication mechanisms should force the user to change from their default assigned password to a new one at first login to the system and after a password reset.

	• Authentication mechanisms should be configured to allow a maximum of 5 attempts to enter a password, after which the user's account should be automatically locked against access for a period of 30 minutes. After 30 minutes access to the account should automatically be re-enabled. • All mechanisms for assigning or changing passwords should be set to automatically apply the rules described above and in addition ensure that the previous five passwords from the password history cannot be used. • 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. Password safes (such as KeePass) may be used for password transmission and storage. 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. • Defined procedures must be followed when communicating default passwords to computer users – see 'Communicating passwords to users' below. • Additional defined policies and procedures are to be followed for the storage and handling of system administrator passwords. **Server administrators (including domain administrator and root accounts)** • 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, the following guidance should be adhered to. • All system administrator account passwords (including domain administrator and root accounts) should adhere to the password assignment rules as defined above 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.

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

	• 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. • Additional security is required for system administrators of critical systems within the scope of PCI DSS and those processing personal data. Tiered accounts should be used to separate system administration and development environments from desktop environments. • 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. • 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** • 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. • 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. • 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. • Desktop local administrator account passwords should only be used where privileges as described above are insufficient to resolve a problem, and direct access via the local administrator account is essential. In such cases, the following guidance should be followed. Procedures should be in place to ensure that the password is only distributed to authorised IT support staff and a log is maintained of those who have access to the password. • Staff (including IT support staff) requiring local administrator privileges on their office computer will have to request this from the IT support manager for their department and give justification for this. Local administrator privileges will only be granted for a finite period of time.

	• The local administrator account password on a desktop system should adhere to the same password assignment rules as applied to servers and defined for server administrators. • 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. • 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. • 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. • 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. **Communicating Passwords to Users** These basic procedures should be followed when communicating passwords to users, either to new users, or when dealing with incidents where a password change has been required and this needs to be communicated to the user. • Only those staff authorised to do so should communicate passwords to users. For ITCS managed IT accounts, such as the UEA IT account allocated to all staff and students, only IT Service Desk staff should inform users of their password following separate additional detailed procedures documented in Service Desk operational documents[2]. • Other staff authorised to inform users of passwords, such as IT support staff allocating passwords for accessing local departmental IT resources where authentication is not controlled by centrally managed Active Directory processes, or course administrators who have been allocated a batch of visitor IT accounts by ITCS for distribution to attendees, should follow the procedures below: o Wherever possible the user should be informed of the password by face to face contact. Before informing the user of the password, their identity should be checked[3].

[2] Service Desk operational documents are stored on the ITCS intranet with access restricted to the Service Desk and other authorised ITCS staff.

[3] Where the user has been allocated a campus card they can be checked against the photo on the card.

	o Where face to face contact is not possible, the user's password should be communicated to them over the telephone after asking them to confirm their full name, their staff or student number, and at least one other piece of information that has previously been collected as part of the authorisation process such as date of birth or home postcode. o The password should be communicated to no other person other than the user, and the user should be reminded that they must keep the password secure and must not under any circumstances disclose it to any other person. o Wherever possible the resource/facility being accessed should be configured to force a change of password when the user first accesses the resource/facility[4] and after every occasion that the password is reset. If this is not possible/practical, they should be instructed to change the password at the first opportunity. o Passwords should never be sent via email or any other digital communication mechanism to recipients.

[4] Enforcing a change of password when first accessing the facility will depend on the type of facility being accessed.