Access Control Policy

Version Control

Version	Date
Draft 0.1	25/09/2017
1.0	01/11/2017

Related Polices

- Information Services Acceptable Use Policy
- Associate Accounts Policy
- IT Security for 3rd Parties, Suppliers and Support Organisations Policy
- Data Storage and Remote Working Policy
- Password Usage and Management Policy

1. Introduction

1.1. Background

The ever-increasing use of digitised and networked information at the University intensifies the risk of data being copied or stolen, or modified, hidden, encrypted or destroyed. Unless access to our systems is appropriately managed, there is an increased risk that unauthorised persons will obtain use of our resources and gain access to University data.

Although technical controls provide an essential element of overall protection, they only deliver a percentage of the required solution, the most effective defence being achieved through awareness and good working practices.

This document forms the University's Access Control and Account Management Policy. It concerns the use and management of logon credentials for University IT accounts (usernames and passwords), extending to the management of third party access to accounts and data. This policy is a subordinate of the Information Services Acceptable Use Policy.

Compliance with this Policy will enable consistent controls to be applied throughout the University, minimising exposure to security breaches, whilst allowing systems administration and technical support staff to conduct their activities within the framework of the law.

Related Policies

- Information Services Acceptable Usage Policy
- Password Usage and Management Policy
- Associate Accounts Policy

2. Creating, Controlling and Managing User Accounts

2.1. Account Creation

User accounts for any IT system will only to be created on the correct authority. It is the responsibility of the system administrator who is creating user accounts to confirm that the correct level of authority has been granted.

2.2. Conditions of Acceptance

The Information Services Acceptable Use Policy is a subordinate policy of the conditions of employment and the student terms etc. As such breach of this policy will be handled by the appropriate processes governing staff or students breaches of contract.

2.3. Identification, Authentication and Traceability

All users of University systems must be identified and authenticated as a valid user prior to access being granted to computer resources, allowing activities performed traceable to individual account holder

2.4. Account Privileges

Account profiles and privileges are to be restricted to the minimum required for individual account holders to fulfil their role.

Access to operating systems and application management is to be restricted to designated administrators and support staff associated with the management and maintenance of the respective platforms.

User privileges are to be reviewed on a regular and frequent basis with an annual access control audit, and withdrawn where the circumstances of those who have been granted privileges no longer warrant such access.

2.5. Staff Account Management

2.5.1 Currency

User-accounts are only to remain active for the period required for individual users to fulfil the needs for which they were granted.

2.5.2 Management of Local Systems Accounts

Staff who administer access to their own systems, not authenticated by Active Directory, are to arrange with Human Resources/Student Administration to receive notification when members of staff or students either leave the University or transfer to a role that no longer requires access to that system.

Administrators are to implement a process for disabling user accounts when the account holder has left University or transferred to a role that no longer requires access to that system.

2.5.3 Closure of Central Accounts

The central IT accounts of paid members of staff will be disabled when the user's leaving date has passed on the central HR system or sooner, if requested by Human Resources.

Upon HR setting the member of staff's leaving date on the central HR system, an email will be sent to the user and their line manager advising them to arrange access to any data that we be required by their colleagues after they leave. Advise can be sought from the IT Services Helpdesk on the best ways of doing this.

55 days after the user has left the organisation, their former line manager will be send a reminder to retrieve any data from the user's account by arrangement with the IT Helpdesk.

60 days after the user has left the organisation, their account and data will be deleted.

It is the responsibility of departments to notify the IT Services Helpdesk when the IT accounts of visitors, those with associate accounts, 3rd party technical support organisations etc. are required to be deleted. However, IT Services will review

such accounts for activity every six months. If they have not been used within the previous six months they will be deleted.

2.5.4 Disabling of Central IT Accounts

IT Services will disable the central IT staff accounts only when requested to do so by Human Resources. Accounts that are disabled will remain 'locked' until the correct University authority informs IT Username Administration that they can be reinstated.

2.6. Student Account Management

2.6.1 Termination of student accounts

Undergraduate accounts will be deleted 180 days after the end of their course.

2.7. System and Service Account Management

2.7.1 Use of Service and System Accounts

Some Corporate Systems, particularly those requiring access to databases, require accounts to be created to run system services or access database tables. The use of generic accounts must not be used for this purpose and specific accounts should be created where needed. Passwords to these accounts should be manged in accordance with 2.5.3 of the *Password Usage and Management Policy.*

Service and System Accounts should be treated as any other and only granted access to the areas of the system required to allow it to function as designed.

2.7.2 User access to Databases

An individual who requires direct access to a database or set of database tables, should only do so via their own Active Directory account with appropriate permissions set so that they only have access to the data they need to fulfil their role.

3. Use of Accounts

3.1. Account Restrictions

You may only use computer accounts that you have been officially authorised to use. Using a computer for which you have not been given permission to use can constitute a criminal offence under the Computer Misuse Act 1990.

Account holders must not divulge their logon credentials to anyone else or allow any other person to use their computer account at any time, regardless of whether the other person is a member of the University.

Any misuse of a computer account may be attributed to the account holder in the

first instance.

3.2. Access Parameters

In accordance with the Use of Computer Systems Policy users must not attempt to access systems, applications or data which their user account does not naturally provide access to and for which they have not been granted specific permission.

4. Controlling Shared and Other Accounts

4.1. Conference Accounts

Where conference and visitor user-accounts are used a custodian in the respective department is to be designated as owner of the accounts and is responsible for their security, allocation and lapsing.

User accounts are only to be issued to conference delegates and visitors when the intended recipients have signed a copy of a form to confirm that they will abide by the Use of the Information Services Acceptable Use Policy. Once signed, forms are to be retained for a period of 12 months after the user has left, and presented to auditors or IT staff on request.

User account custodians are responsible for notifying the IT Services Helpdesk of the date requirements as they issue these accounts, or for emailing an account expiry request to helpdesk@leedstrinity.ac.uk when the users no longer require access to University systems.

4.2. Associate Accounts

The University has provision for the creation of Associate Accounts. An Associate is someone who needs access to the University's IT services and who does not gain it automatically by being in the University's HR or Student Record systems. There are a number of different roles which fall into this category, for example contractors, visiting lecturers, consultant IT staff, suppliers and 3rd party support organisations. The *Associate Accounts Policy* should be refereed to, however the provisions of this policy still apply.

5. Third Party Access to Email and File Stores

5.1. Allowing Others to Access Your Email

Members of staff are to assign delegated rights to their mailbox if they have a need for someone else to access their email, for example, secretaries on a permanent basis, or staff covering a particular role during periods of temporary absence.

5.2. Sharing Your Data

Where there is a requirement to share access to your files, this should be done through the Leeds Trinity provided OneDrive for Business service, with the

appropriate sharing permissions set for the intended recipients.

5.3. Third Party Cover Arrangements for Known Absence of Staff

When a school or department knows that a member of staff is going to be absent from work, and that for operational reasons access will be required to either their email account or file store during their absence, they are to make arrangements in advance of the absence in accordance with 5.1 and/or 5.2 above as appropriate.

5.4. Management Third Party Access to Email and Data

All third-party access to other users' data in their absence must be justified for operational purposes and fully accountable. The processes for gaining third party access to a user account are defined in the Access Control and Account Management Standard.

5.5. Third Party Access during Unexpected Staff Absence

Where a member of staff is unexpectedly absent from work and it was not practical for advanced access arrangements to be made before their absence (see 5.3) IT will, on the correct authority, facilitate third party access to the required email account or file store.

On signing the third party access application form management and staff agree to adhere to the terms and conditions of access.

5.6. Approval and Authority - Third Party Access during Unexpected Staff Absence

Approval for third party access to an account when a member of staff is unexpectedly absent from work must be provided by the appropriate head of school / head of service.

If a head of school requires personal third-party access to the data of one of their staff, the application form must be authorised by their line manager.

Following approval of the application the Director Information Services, or in his absence the Head of IT Services, must provide authority before IT staff facilitate the required access.

Completed application forms will be retained by IT Services for a period of two years and will be made available to auditors or the IT Security Team on demand.

5.7. Third Party Restrictions

Anyone who is granted operational access to another users' data may only view material that it is considered necessary to see for the operational reason for which access was granted. They are required to treat all material as confidential and not to act upon it or disclose it to any other person except those directly associated with the operational requirement for which the access was granted. In addition, they must preserve the confidentiality of any private or personal data that they

may view inadvertently whilst undertaking operational matters. On signing the 'Third Party IT Account Access Form' the person who is to be provided with the access to another users' account is certifying that they have read and understood the requirements.

5.8. Control and Accountability of Student Accounts

Access to students' files must be restricted to bone-fide reasons, such as, investigating plagiarism or malpractice, or to verify that existing work space is not being used for the storage of non-work related material where more disk space is requested. If there is any doubt as to whether access to a student's files is bone-fide, the head of the school is to be requested to provide the required authority.

Any person viewing a student's accounts must do so in the presence of a second person e.g. a lecturer with a member of IT staff, or two IT staff. A written summary as to why this was done and what the outcomes were must be produced and a copy of this is to be given to the student as well as being kept on their file.

6. Dealing with Misuse, Abuse and Illegal Activity

6.1. Requests for Account Access by the Police and Law Enforcement Agencies

All requests from the police and other law enforcement agencies for access to computer information or user accounts must be directed to the Secretary to the University or in their absence, the Chief Operating Officer.