UNIVERSITY OF CAMBRIDGE
Finance Division

University of Cambridge Financial Systems

CUFS User Policy

The purpose of this policy is to establish security and privacy access requirements and standards to ensure acceptable use of information technology resources and integrity of the University's enterprise financial data and systems.

Authors:	Jo Hall		
Version:	V5.0	**Date Created:**	17th December 2013
Status:	Approved	**Date Last Updated:**	12th September 2018
Document Location:	R:\UFS\2. System Support\1. Systems Support Framework\2. CUFS User Policy\CUFS User Policy v5.0 Approved 22 May 15 updated 12 Sep 18.docx		

UNIVERSITY OF CAMBRIDGE
Finance Division

Document Control Details

Amendment History

Version	Status	Date	Author(s)	Summary of Changes
0.1	Draft	17th Dec 13	Allison Benton	First draft
0.2	Draft	17th Dec 13	Allison Benton	Updated with feedback from Chris Patten
1.0	Issued	3rd Feb 2014	Jo Hall	Updated and formatted for issue
2.0	Revised	1st Sept 14	Jo Hall	To add Administrator, Functional, Developer, DBA access
2.1	Issued	21st Oct 14	Jo Hall	Updated with actions from meeting 21st Oct 14
3.0	Final	17th Dec 14	Jo Hall	Updated with final certification on access from CE
3.1	Final	6th Jan 15	Jo Hall	Updated for approval by Michelle Finnegan
4.0	Approved	27th May 15	Jo Hall	Updated with feedback from meeting 22nd May 15
4.1	Approved	16th Oct 15	Jo Hall	Spelling corrections
4.2	Approved	29th Oct 15	Jo Hall	Amendment to 3.3 CUFS Training
4.3	Approved	12th Sep 18	Michelle Bond	Amendments to 4.2 and 4.5 for passphrase policy
5.0	Approved	5th Aug 19	Jo Hall	Update headers and footers for version control

Reviewers

Name	Role	Date Complete
Jo Hall	Head of Financial systems	21st Oct 14
Chris Patten	Head of Accounting Services	21st Oct 14
Steve Hutson	Deputy Director, Finance Division	21st Oct 14
Chris Edwards	Deputy Director, UIS	21st Oct 14
Mark Galvin	Systems Assurance Manager, UIS	21st Oct 14
Shaun Lindsey	Team leader, Application and Database Administration, Operations Support	21st Oct 14
Mark Ansell	IT Operations Manager, Operations Support	21st Oct 14
Phil Taylor	Senior Developer	21st Oct 14

Approvals

Name	Position	Date
Chris Patten	Head of Accounting Services	22nd May 2015
Steve Hutson	Deputy Director, Finance Division	22nd May 2015
Mark Galvin	Systems Assurance Manager, UIS	22nd May 2015
Mark Ansell	IT Operations Manager, Operations Support	22nd May 2015
Michelle Finnegan	Assistant Director of UIS, Strategy and Administration	22nd May 2015
Phil Taylor	Senior Developer	22nd May 2015

Contents

1 Policy 4
1.1 Policy Statement 4
1.2 Reason for Policy 4
2 Financial System 5
2.1 Oracle Financials 5
2.2 Retention of Information 5
2.3 Sharing of Information 5
2.4 Accessing Information 6
2.5 Data Protection Act 7
2.6 Freedom of Information Act 7
3 Access Control 8
3.1 Key Contacts 8
3.2 Access 8
3.3 CUFS Training 8
3.4 Non Employees/Students 8
3.5 Responsibility Changes 9
3.6 Amendments to CUFS Accounts 9
3.7 Records 9
3.8 CUFS Audit 9
4 UFS Security 10
4.1 Segregation of Duties 10
4.2 Access to the desktop (PC; MAC etc.) 10
4.3 User Accounts 10
4.4 Disabled Accounts 10
4.5 Passphrases 11
5 Transactional Processing 12

1 Policy

1.1 Policy Statement

The University has been entrusted with public funds to fulfil its mission of education, research, and public service. All University faculty and staff under the leadership of its officers are obligated to ensure that University funds are used only for mission-related purposes.

Leadership responsibilities for fiscal control include assurances that the following exist:

- Documented policies and procedures;
- Staff are properly trained for their assigned duties;
- Mechanisms to ensure compliance with policies.

All University personnel are responsible for ensuring that fiscal controls exist and are used to prevent abuse or misuse of University funds and other resources.

Should a breach of this policy be identified or suspected this should be referred to the Finance Director as owner of the Finance System.

This policy can be found on the Finance Division webpage at: http://ufs.admin.cam.ac.uk/

1.2 Reason for Policy

The purpose of this policy is to establish security and privacy access requirements and standards to ensure acceptable use of information technology resources and integrity of the University's enterprise financial data and systems. This policy is intended to ensure that:

- Authorised individuals are granted appropriate system access to perform their duties while minimising the risk of the financial data or systems being compromised.
- Authorised individuals properly use the enterprise financial data and systems.
- Authorised individuals properly maintain privacy and confidentiality of financial data and systems.

2 Financial System

2.1 Oracle Financials

The University uses a software package called Oracle Financials to record financial transactions and to provide the data necessary to compile its accounts. It has been in use since August 2000.

The system is widely referred to as CUFS (Cambridge University Finance System) or UFS (University Finance System).

CUFS offers “real time” processing, meaning that you are able to obtain a true picture of the financial position at any given time. The system records financial budgets, money coming in, going out and any commitments to spend. Different tasks can be performed in different areas of the system and each area is known as a module.

Reliable financial information is essential to effectively manage the business of the University and protect its assets. A strong enterprise financial system management program is necessary to ensure the integrity of financial information. To maximize the value of the University's enterprise financial information, the University will:

- assign and clearly define responsibility and accountability for protecting the financial systems and its data against unauthorised use.
- enforce compliance with security and privacy laws, requirements, policies, procedures, standards, controls and security incident reporting and response.
- promote security measures that will maintain the integrity, confidentiality and availability of the data and systems.
- participate in a University-wide Security and Privacy Awareness Program.

Proper use of financial data and systems will be consistent with University mission, policies, and procedures. Inappropriate use, collusion and vandalism will be prosecuted by the University to the full extent that the law will allow.

2.2 Retention of Information

Financial records must be retained in accordance with the Retention, Archival and Destruction of Records policy and schedule.

2.3 Sharing of Information

Under the Data Protection Act 1998 the University has a legal responsibility not to share data if it knows that the data will not be handled correctly nor to receive and use data if it has not been collected properly.

2.4 Accessing Information

The Rules imply that all information held in a computer facility is prima facie confidential unless obviously intended for unrestricted dissemination. No-one should attempt to access information unless he or she has explicit or implicit permission to do so.

Implicit permission may, for example, consist of a reference in a manual or other documentation to the contents of a particular file. It is particularly important to note that the fact that information may be readable (or even alterable) does not in itself imply permission for it to be read.

Some files (for example those called /info, etc.) may be available for public scrutiny, but browsing through file spaces is not generally permitted. Information in transit on a network is similarly confidential and the unauthorized monitoring of network traffic is explicitly forbidden.

Nevertheless, users need to be aware that their communications may be intercepted by IT staff as permitted by UK legislation. The legislation allows the interception of network traffic without consent for purposes such as recording evidence of transactions, ensuring regulatory compliance, detecting crime or unauthorized use, and ensuring the efficient operation of University communications systems.

The University Information Service does not need to gain consent before intercepting for these purposes although staff and students do need to be informed (via documentation such as this) that interceptions may take place.

University Information Service staff responsible for the management of systems may, in the course of their duties, need to bypass normal protection mechanisms in order to access user files or jobs, either to trace a system problem, or to monitor possible system abuse.

Staff may also suspend authorization when abuse of a system is suspected. Established procedures are followed and staff are required both to record their activities, and to maintain the confidentiality of any scanned material.

Data stored on Service systems is regarded as the property of the owner and will not usually be released to a third party except with explicit permission. However, if there is evidence of criminal activity or abuse of the system, confidential material may be released at the discretion of the Director of the University Information Service.

All access to "personal data" (i.e. information which relates to a living person) must be covered by an appropriate registration under the Data Protection Act, 1998. See the Act itself for the full description of "personal data". Anyone who is considering keeping such "personal data" on a University Information Service machine MUST seek advice from the University Information Service before installing the data

The unauthorised access of data and its manipulation, corruption or destruction – regardless of whether or not this is for personal gain – will be treated as a serious offence. Appropriate action will be taken against individuals who misuse data. It is illegal to disclose unauthorised data held on a computer to a third party. Unauthorised disclosure of any such information may, therefore, lead to disciplinary action being taken.

2.5 Data Protection Act

Record keeping must comply with the Data Protection Act 1998.

CUFS is not deemed to hold what would be classed as “sensitive data” under the data protection act.

2.6 Freedom of Information Act

The University is subject to the Freedom of Information Act 2000 and members of the public may request copies of University documents. Advice on these matters must be obtained from the University’s Data Protection and Freedom of Information Officer.

3 Access Control

3.1 Key Contacts

Within each Department of the University there will be a CUFS Key Contact, who is nominated by the Head of Department. Key contacts are responsible for all aspects of CUFS user accounts in the LIVE (production) system (with the exception of System Administration level access to support the application and database)

Key Contacts provide an essential part of the management of the CUFS and serve as the liaison between the University Finance System Group (FSG) and the Department.

Key Contacts maintain the departmental list of UFS roles and responsibilities, and ensure that requests for changes are submitted using the on-line forms available on the Key Contacts web page. They will ensure that only responsibilities which are necessary for the user's business, function within the University, are requested.

3.2 Access

Initial access rights to CUFS and any subsequent modifications to user rights/permissions should be formally requested and authorised via the Key Contact (with the exception of System Administration level access to support the application and database)

Users are not allowed to authorise their own access requests.

Access rights/permissions should be sufficient to meet the minimum requirements for the user's role, but not unreasonably exceed the level of authorisation necessary to perform legitimate job functions.

3.3 CUFS Training

Key Contacts should ensure that all users receive the correct training for their CUFS access.

iProcurement, AP Invoice Entry/Manager and AR User/Manager responsibilities will not be given until minimum levels of training has been completed.

Other module courses such as General Ledger and Grants are available and highly recommended. A full listing of CUFS courses are available on the Finance Training website. These courses include all the basic steps required for users starting out in CUFS and are often available in an online format.

Managers of the University are obligated to ensure their staff are trained in appropriate use of the system.

3.4 Non Employees/Students

In order to grant access to CUFS to students / non-employees a registered CUFS Key User must validate the application. This validation confirms the CUFS Key User has made the Student / Non-Employee aware of and explained the statements in Section A of the form.

Key Contacts requesting new CUFS access for students / non-employees should arrange for the students / non-employees to complete the CUFS Access – Finance Division form before requesting access.

3.5 Responsibility Changes

If a user's job role changes, the user's responsibilities must be reviewed and the user's responsibilities be removed or modified as appropriate. Additional responsibilities can be added or existing responsibilities removed by using the Users responsibility changes form.

3.6 Amendments to CUFS Accounts

Details of staff leaving the department, no longer requiring access or requesting more responsibilities must be submitted using the responsibility change form on the Key Contacts web page. This will also help the audit process.

Responsibility forms should also be used for notification of staff on long term sick or maternity leave so the accounts can be disabled until their return.

This is an essential element of the security procedures appertaining to CUFS.

3.7 Records

The CUFS system records all user actions; this is in accordance with government financial regulations. Therefore it is not possible to remove/delete a user; only to disable those users' CUFS access/responsibilities. Hence user responsibilities (except Purchasing Limits, which are removed), are end dated, not removed.

3.8 CUFS Audit

Twice a year the Responsibility by Department report is sent to all department Key Contacts to review, confirm and sign off.

4 UFS Security

4.1 Segregation of Duties

A fundamental element of internal control is the segregation of certain key duties, in order to ensure that no-one is in a position both to perpetrate and to conceal errors or fraud in the normal course of their duties. To reduce chances for fraud and facilitate financial data accuracy, the following tasks should be assigned to different individuals:

- authorising the use or exchange of assets (cash, payroll, purchasing)
- handling assets (stocking inventory, distributing checks)
- recording transactions (accounting).
- ordering and invoice approval functions

If staff limitations compel one person to have these responsibilities, management must accept responsibility for monitoring and verifying transactions to help ensure financial data integrity and protection of University assets.

4.2 Access to the desktop (PC; MAC etc.)

CUFS Users are first required to logon to the University network via a network logon containing the CRSid as a username and a passphrase selected by the user. This passphrase will not expire.

Once logged on individuals must ensure that they lock their PC / MAC etc. while unattended.

It is the user responsibility to ensure that their computer is up to date with software updates and protected by suitable anti-virus / malware software.

4.3 User Accounts

CUFS accounts are for the named user only. The Key Contact must make this clear to all users within the department.

If for any reason it is suspected that access has been given to anyone other than the named user, the account will be deactivated while the situation is investigated.

The Key Contact will be informed if this issue arises.

4.4 Disabled Accounts

Accounts will be disabled if not accessed for a period of 120 days or more.

For users that do not use the system on a regular basis it is advisable to access the system occasionally to prevent the account being disabled.

A disabled account can only be re-enabled on at the request of the Key Contact by submitting a responsibility change form.

Accounts will also be disabled if it is thought that the account has been used inappropriately.

4.5 Passphrases

Users can submit a form requesting a new passphrase. This does not have to come from the Key Contact.

The online form is available on the UFS front page under Passphrase Problems: http://ufs.admin.cam.ac.uk/

Users should ensure they keep their passphrases and user names secure and do not share them.

Users are advised that their passphrase word should be easy for them to remember but difficult for others to guess and should contain.

The first time a user accesses CUFS they will be prompted to change passphrase.

- Passphrases must be a minimum of 13 characters.
- To create a strong passphrase, it is strongly recommended that it combines three random words that have meaning to the user that would not be easily guessed.
- The first time a user accesses CUFS they will be prompted to change ‘passphrase’. Valid characters are letters, A through Z and numbers, 0 through 9.

Usual recommendations and wording relating to passphrases apply as published by the University Information Service.

Users are not required to change their passphrases.

5 Transactional Processing

Individuals initiating transactions are responsible for obtaining proper authorisation.

Transactions must be recorded accurately, in a timely manner, and completely within financial system guidelines and applicable external organisational rules (including organisations funding University programs and the HMRC), to ensure integrity of the University's financial data.

Accurate recording includes adequate descriptions of transactions, as well as the correct use of chart of account codes.