Use of *EASE*
Code of Practice

Introduction

This code of practice is intended to support the Information Security Policy of the University and should be read in conjunction with this document.

http://www.ed.ac.uk/schools-departments/information-services/about/policies-andregulations/security-policies/security-policy

This code of practice is also qualified by The University of Edinburgh computing regulations, found at:

http://www.ed.ac.uk/schools-departments/information-services/about/policies-and-regulations

1. Code of Practice Version

[The CoP for any system is expected to develop over time. For this reason, it may be important to track versions of any CoP. This section in the template suggests a framework in which you could record reasons for change to the CoP for the system referred to.]

Revision Date	CoP Version	Template Version	Author	Notes
4/10/11	1.1	1.0	Graeme Wood	Initial document
29/9/14	1.2	1.4	Graeme Wood	Adopting template
6/11/14	1.3	1.4	Graeme Wood	Minor edit

QA Date	QA Process	Notes
15 Dec 2014	ITC Sec Working Gp	

Suggested date for Revision of the CoP	Author
September 2016	Graeme Wood

2. System description

Revision Date	System Version	Author	Notes
29th September 2014	Cosign 3.0.2/ MIT Kerberos	Graeme Wood	Current version of Cosign and Kerberos in use

	1.12.x		

2.1	System name	EASE
2.2	Description of system	EASE provides a reduced sign-on service to University services through the use of a Kerberos KDC and a web sign on service using Cosign.
2.3	Data	Identity information to allow the creation of accounts is supplied by the Identity Management service (IDM).
2.4	Components	There are four resilient web login servers and two resilient Kerberos KDCs. The identity information database allowing the initial registration of usernames and passwords is provided on a resilient pair of database servers.
2.5	System owner	The service is provide by the Unix Section of the IT Infrastructure division of Information Services.
2.6	User base	All users of University services can use the EASE service to authenticate. This includes guest users who can self-register using their own personal email address.
2.7	Criticality	High.
2.8	Disaster recovery status	All components of the service are replicated and resilient and will automatically cope with the failure of any one component. The master password server requires manual failover to the resilient server via a DNS update. The DR process has been well-tested.

3. User responsibilities

3.1 Data	It is important that a good password is used. Users should refer to the published guidance on setting a strong password. Passwords should be changed on a regular basis, but not so frequently that it becomes difficult to remember what the password has been set to. EASE passwords should never be written down. Users should never save their password in their preferences or settings for their application e.g. Internet Explorer, Firefox or Outlook unless protected by a keychain and strongly encrypted. These preference files are often stored on network attached storage and are not strongly encrypted. Unless the EASE account is explicitly for a shared purpose, such as a functional account, EASE passwords should never be divulged to anyone and especially not in response to an email message. IS and other University staff will never ask for an EASE password. When setting passwords for services other than EASE, and Active Directory (AD) which is synchronised to EASE, the EASE password should not be used. For example, less secure services such as the University's web proxy service should always use a different password to EASE. This is because these services have a lower security level than EASE and AD and a compromise of the password for those services should not have any impact on the security of EASE. Users should not enter their EASE password into any dialogue box or password prompt unless it is on the EASE web-login website, or a service that has been explicitly advertised as using EASE e.g. staffmail, SMS or desktop logins. Users should check with the service documentation or their computing support staff if they are in doubt as to what services use EASE. Users should never enter their EASE password into any website other than the EASE website. Users should ensure that their computer is clean of viruses and other malware. A common method of compromising passwords is for a virus or download to install a keyboard sniffer that captures keystrokes as they are typed. It is therefore important to install and maintain adequate virus protection software appropriate to the platform in use.

3.2	Usernames and passwords	Members of the University, applicants to the University and official visitors are entitled to an EASE account and will be provided with a University Username (UUN) and a single use registration password. This allows them to set their own EASE password and register shared secret information, which may be used later to confirm identity or allow self-service password reset in case of a forgotten password. When registering an EASE account it is important that only the account holder registers the account. This ensures that proper registration of shared secret information is completed. People other than the above categories may register their own EASE Friend account. Such accounts have a lower level of security and are only used for access to certain web services. EASE Friends do not register shared secrets. Nevertheless EASE Friends should ensure the security of their EASE password by adopting the same practices described below.
3.3	Physical security	If users have a mobile device which has saved/cached their EASE password then they should ensure the device is kept secure and is appropriately locked when not in use. Any device that is lost or stolen should be remotely wiped if possible and users should change their passwords.
3.4	Remote/mobile working	EASE supports remote and mobile working.
3.5	Downloads and removal of data from premises	Identity data is restricted and cannot be downloaded from the service.
3.6	Authorisation and access control	Access to some parts of the EASE web login servers are restricted. Access control is done by use of .htaccess files and named accounts and by using data from the Central Authorisation service using LDAP.
3.7	Competencies	Users should not divulge their passwords to any third-party.

4. System Owner Responsibilities

4.1 Competencies	All service providers should ensure that their systems are well-managed and up-to-date with security patches, and that appropriate virus protection software and firewalls are utilised to protect their service appropriate to the platform used. The EASE servers and the EASE Kerberos key distribution centres are appropriately managed to keep them secure. The EASE web site and Kerberos KDCs are well maintained and patched.

4.2 Operations	The code of practice is designed to limit the transmission of users' EASE passwords over the network, even over encrypted connections. It is recognised however that sometimes this is unavoidable. The suitable situations where users' passwords are entered over a network are described below. Web service providers should never construct their service so that it prompts directly for a user's EASE password in order to authenticate. Web service providers must use the approved cosign software, which can be downloaded from the EASE website. Do not under any circumstance embed an EASE password prompt in a web page or design a web page to mimic that of the EASE web-login website. All web service providers using EASE are required to register their service with IS in order to make use of the service. Since EASE provides an authentication service to people outside the University, such as visitors, alumni or anyone registering as an EASE Friend, it may not be appropriate to assume that because someone has authenticated to EASE that they should have access to an EASE protected resource. Web service providers using EASE should ensure that appropriate authorisation is in place to secure access to web resources. Such authorisation systems may include .htaccess files or the University's Central Authorisation Service. EASE provides mechanisms to support delegated authentication by provision of either a Kerberos ticket, or to allow web services to act as proxies for other services using EASE. The provision of Kerberos tickets to web service providers would not normally be supported to services outside Information Services, but may be supported by special application where extra assurances of security and trust are provided. The permission to support EASE protected websites proxying for other websites is permitted provided that permission is given from the website owners whose services will be being proxied by the proxy service. EASE also provides a two-way trust relationship to the other Kerberos realms in the University provided by Active Directory and the School of Informatics. No other trust relationships are permitted. Non-web services may also use EASE. However the services must first comply with one of the following: ■ They must work using the standard Kerberos GSSAPI protocol to authenticate using an EASE Kerberos ticket granted by the EASE Kerberos service. It is therefore permissible for service providers to configure end-user systems to be part of the EASE Kerberos realm and allow users to enter their username and EASE password in a desktop login or by the use of kinit or equivalent. ■ In some exceptional cases applications may be allowed to prompt for an EASE password even when the application is accessed over a network. The application developer must ensure that this cannot happen over an unencrypted connection. Any network communication of passwords must be secured using Transport Layer Security (TLS) or Secure Sockets Layer (SSL) protected using certificates whose key length is at least 2048 bits. Service providers must first seek approval and vetting of their application design from IS before use of the service in this way will be permitted. Such applications may be subject to further vetting by Internal Audit

4.3	System documentation	Documentation on the use of EASE is available on the IS website and on the EASE website. Documentation on the management of EASE itself is held on the ITI Unix Section wiki.
4.4	Segregation of Duties	Service owners need to ensure the security of their services and that they are using up to date versions of the Cosign web sign on software as provided from time to time by IS. The ITI Unix Section maintain the security of the EASE servers and Kerberos KDCs.
4.5	Security incidents	Any security incidents related to the firewalls would be referred to the IS IRT, who would log the issue and aid with investigation. Any security incident related to the firewalls would be reported to the ITI Unix Section head who would appropriately report to the ITI Director.
4.6	Fault/problem reporting	Any faults would be raised by the service owners of end user services or by ITI Unix Section staff. If necessary support calls are logged with end suppliers via maintenance contract.
4.7	Systems development	The cosign and Kerberos software is open source software maintained elsewhere. Local scripts and web page design is carried out by ITI Unix Section technical staff.

5. System Management

5.1	User account management	A small number of local system logins are provided for administration. These are only granted to members of the ITI Unix Section with appropriate skill set.
5.2	Access control	Only ITI Unix Section staff have access to the EASE servers and these servers are protected with local firewalls and the FWSM central firewall.
5.3	Access monitoring	All logins are logged locally on each server and centrally on a log server.
5.4	Change control	Change management is organised through the ITI Unix Section service management procedures. Any major change – e.g. major firmware revision or change in platform - would be discussed and scheduled with end service providers and communicated through IS alerting processes.
5.5	Systems clock synchronisation	All servers synchronise their clocks to UTC using the NTP protocol.
5.6	Network management	Management of the networks that these servers are connected to is provided by the ITI CIS.
5.7	Business continuity	The EASE web login servers and the EASE Kerberos KDCs are fully replicated and resilient and are placed in multiple sites. Disaster recover testing takes place regularly.
5.8	Security Control	Access to the servers providing EASE is strictly controlled and physical access is maintained in the IS data centres. End-users have no access to the EASE servers.

6. Third Party

6.1	Outsourcing	N/a.
6.2	Contracts and Agreements	Hardware support contracts are in place with Oracle and Dell.
6.3	Compliance with the university security policy	The hardware support contracts with Oracle and Dell do not permit access to the services. The agreements comply with the university's security policy.
6.4	Personal data	No personal data is exported.