Use of *The Information Services' Active Directory Service (AD)*
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
25/10/2011	0.1	1.4	Martin Cassels	Initial Draft Sections 1-4
27/10/2011	0.2	1.4	Garry Scobie	Section 6 Initial Draft
14/11/2011	0.3	1.4	Martin Cassels	Sections 4 ,5 & 6.4 Initial Draft.
16/03/12	0.4	1.4	Garry Scobie	Additions to sections 3.6, 4.4, 5.2, 5.3, 6.2, 6.3
18/05/12	0.5	1.4	Garry Scobie	Minor grammar and clarification changes to sections 2.4, 2.8, 3.2, 3.6, 3.7, 4.4, 5.2, 5.6, 6.3
21/08/14	0.6	1.4	Garry Scobie	Added ADFS and O365 to section 2.4. MS contract details updated 6.2. Minor clarifications to sections 4.2, 4.4, 4.7. AD version change Section 2.

QA Date	QA Process	Notes
15 Dec 14	ITC Security WP	V0.6

Suggested date for Revision of the CoP	Author
15 Dec 15	Garry Scobie

2. System description

[This section is intended to give an overview of what the system is, and to ensure that overarching aspects of system security have been considered. If you think that there is any other pertinent information to provide about the system here in addition to the subsections below, please add it into this section.]

Revision Date	System Version	Author	Notes
25/11/2011	2012	Martin Cassels	Initial Draft

2.1	System name	Active Directory or AD
		Active Directory provides an Authentication, Authorisation and LDAP Directory service.
2.3	Data	AD stores user's identity information (see separate sheet for details), department information and to a certain extent the structure of the Universities' organisational hierarchy. It also stores groupings of users, systems and authorisation details for them to enable or block access to various systems.
2.4	Components	The core Active Directory service consists of a number of servers known as Domain Controllers (DCs) and a Certificate Authority Server (CA). The Directory itself is split into two separate Domains 'Edinburgh.ac.uk' and 'ed.ac.uk' both of which are driven by proprietary Microsoft Jet Databases replicated to all domain controllers in the domain the DC serves. The CA provides internal certificates to allow encrypted LDAP access to the directory over Secure Socket Layer protocols (SSL) by core services and by end-user computers including many running non-Microsoft Windows operating systems. Active Directory Federation Services (ADFS) is deployed to facilitate the provision of Microsoft Office 365 for email and diary which is hosted externally by Microsoft.
2.5	System owner	The system is owned and managed by the Architecture services Team in the IT Infrastructure division of Information Services. The primary contact for general technical enquiries is Martin Cassels.
2.6	User base	AD provides accounts to members of staff, official visitors Students and functional accounts. AD provides directory, authentication and authorisation services University wide.
2.7	Criticality	High

2.8	Disaster recovery status	A Disaster Recovery Plan is in place and has been tested by Architecture Services. The Plan is recorded in the ITI Architecture wiki. There are several scenarios ranging from complete ground up recovery to replacement of individual accounts, groups. The AD service has a great deal of redundancy built in with regard to hardware or communication failure. Higher level incidents such as organisational Unit deletion or database corruption have multiple recovery methods which vary depending on the exact situation ranging from individual object restores to complete restoration of the AD database. Exercise of these recovery procedures requires application of knowledge and experience held by members of the IT Infrastructure team. It is impractical to describe the detailed method for all data recovery situations that may arise.

3. User responsibilities

["Users" includes those who are involved in the administration of the system as well as people who use the system for the purpose for which it was made. When filling in the parts below, you may find you need to describe different responsibilities for different types of user.]

3.1	Data	Staff, Students, Registered Visitors and Functional Identities are entitled to Active Directory Accounts. These are jointly referred to as 'Identities'
3.2	Usernames and passwords	A University Username (UUN) and initial password are assigned to an identity by the central Identity Management system (IDM). This password is available to relevant Computing officers and Helpline operators. The initial password should never be used by the end-user when they register with the University's Authentication Service (EASE). Active Directory Passwords are normally (but still optionally) synced with the EASE password via the facilities that exist for EASE, including resetting a forgotten password via shared secret information. (See EASE code of Practice). 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. Currently there is a minimum password length of seven characters.
3.3	Physical security	Computers and devices using the Active Directory service should be given appropriate security given the information they contain. This will vary from system to system ranging from simply ensuring the system is not lost or stolen to ensuring physical access to the system is restricted in line with the policies set down in the 'Information Security Policy' document. If a computer or device which is registered in Active directory is lost or stolen it is important to inform Information Services via the IS Helpline in order that the device registration can be deleted (or reset) and any AD accounts that have been used on the system have their passwords changed as soon as possible. All computers using the Active directory service should have all reasonable steps taken to ensure they are clean of viruses and other malware. Common methods of compromising passwords are for viruses or malicious downloads/web sites 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

3.4	Remote/mobile working	The policy for mobile working is similar to the guidelines set out in 'Physical Security' but is replicated here for completeness. With regard to remote working it should be noted that when using their own equipment users should ensure that their computer is clean of viruses and other malware. Common methods of compromising passwords are for viruses or malicious downloads/web sites 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. If a computer or device which is registered in Active directory is lost or stolen it is important to inform Information Services via the IS helpline in order that the device registration can be deleted (or reset) and any AD accounts that have been used on the system have their passwords changed as soon as possible.
3.5	Downloads and removal of data from premises	User and device information from Active Directory relevant to the user(s) of the device in question are permitted to be removed from University premises while under the care of an eligible account holder. Caution is advised as above. Mass data acquired from Active Directory using LDAP queries or backups must not leave the University premises (in line with the Information Security Code of Practice.) There are no exceptions to this for users. (Service owners and members of Information Services Infrastructure Division may require to do this when authorised but only in their role as a service provider and not as a 'user'.)
3.6	Authorisation and access control	New users of the Active Directory are provisioned via the University IDM system and a platform provider run by ITI-Architecture Services. The only exceptions to this are accounts created by ITI Architecture services team necessary for system operation. Administration of the UoER area of the directory service is delegated to Schools (dependant on the Organisation code) and IS User Services Division enabling them to implement authorisation and access control to their own systems. Above this ITI-Architecture services manage all authorisation and access control and delegate permissions and rights to Organisations, teams and individuals to systems and resources out with existing delegated administrative structure. Owners of services that use AD may have agreements with 3rd party suppliers and may allow access at the Application layers for support and maintenance functions. Architecture Services do not have knowledge of the details of such arrangements.
3.7	Competencies	Users of the Active Directory are expected to have a basic working knowledge of computers and the particular operating system, PC or device they are using. They should be familiar with the concepts of choosing a strong password, logging on and off from a computer network and an understanding of the risks of virus/malware infection is expected. Advanced users are expected to be proficient in the use of any tools they are using, or to seek training before attempting to use the more advanced features of the directory service.

4. System Owner Responsibilities

[The "System Owner" may be an identifiable person, a post, or the name of a "unit" responsible for the system. The system owner may have created the system, or may have bought/acquired and configured the system. Either way, the system owner is responsible for the underlying security of the system, its platform, the security of its data stores, the initial configuration of the system, and ultimately, for the security of the system throughout it's lifetime]

4.1	Competencies	The ITI-Architecture Services Team owns the Central Active Directory Service. It is one of this team's primary functions is to specialise in Active Directory and ensure all team members have sufficient knowledge and understanding of the concepts, tools, processes, internal operation and security of service to deliver and support an implementation of Active Directory that is highly tailored to the University's needs.
4.2	Operations	The Active Directory Service components (physical hardware, software and data) are the responsibility of the ITI Architecture Services team in conjunction with the ITI Communications Infrastructure Section (CIS), in the case of physical hardware. CIS provide security for and access to the machine rooms where the servers are located. As a major authentication and authorisation service within the University, physical access to the servers is restricted to IT Infrastructure Division teams. Administrative/OS/Service level administrative access is limited to the ITI Architecture Service team.
4.3	System documentation	Active Directory is a product of Microsoft Corporation and to date runs exclusively on its Windows Server line of products and as such is documented extensively not just in Microsoft's documentation and support resources, but in numerous books and Courses ranging from beginner to expert level. It is the responsibility of the ITI Architecture Services team to produce, provide and maintain documentation specific to the implementation of the service within the University of Edinburgh. The level of detail in this documentation is appropriate to ensure the security of the service, and is not to be published on public facing websites.

4.4	Segregation of Duties	Enterprise Administrators and Domain Administrators - Limited to members of the Architecture Services Team and any ITI Architecture owned functional accounts only. All other accounts in the university are standard users with the exception of closely integrated Active Directory Service providers such as Microsoft Exchange who have may have additional access rights to allow them to operate that service. Administration is currently carried out via web based tools provided by ITI Architecture to enable the delegation of rights for specific tasks which normally require elevated privileges. These consist of: 1st Line Support (Library Helpdesk and IS Helpline) 2nd Line Support (IS User Services Division and School COs) 2nd Line and certain delegated configuration responsibilities (IS User Services Service Delivery) 3rd Line Support ITI Architecture Services. Owners of services that use AD may have agreements with 3rd party suppliers and may allow access at the Application layers for support and maintenance functions. Architecture Services do not have knowledge of the details of such arrangements.
4.5	Security incidents	On discovery of a security incident the ITI Architecture Services Team should be contacted immediately via the team telephone number 651 3246. Additionally the incident should be logged with the IS Helpline who will escalate through the various support levels. Computing officers within the support structure discovering an urgent security incident should contact Architecture Services Directly or if necessary the ITI Incident Response Team.
4.6	Fault/problem reporting	ITI Architecture run continuous system health monitoring using Microsoft System Center – Operations Manager which proactively detects issues in many cases, however due to the spread of servers, physical locations and size of the service it is unrealistic to detect all faults pro-actively. On discovery of a suspected fault (where the fault is detected outside the support structure), the user should raise an incident with 1st Line support who will if necessary escalate the incident.
4.7	Systems development	There are development and test environments for the service that mirror the live service in the key areas necessary. A ‘Dev/Sandbox’ environment (devtest.ed.ac.uk) and a test environment (adtest.ed.ac.uk) to be used solely as a pre-production test and deployment environment. All development of the Active directory Service is initially carried out within this environment before deployment to the Live Service. Due to the nature of the service it is possible to create a stand alone workstation based labs for more casual development testing of general Active Directory concepts and services. It should be noted that all environments will undergo occasional overhauls to keep them into line with production.

5. System Management

[Ongoing management of the system has implications for the ongoing security of the system. While some of these matters are dealt with under administrative users above, there are additional responsibilities in managing the system at a lower level.]

5.1	User account management	Active Directory user accounts are created via a coded interface to the University's IDM system. The IDM System manages and dictates service eligibility, and account status for creation, suspension and deletion.
5.2	Access control	Administrative access control is provided and controlled by the ITI Architecture Services Team. Devolved administration via the Web tools for 1st and 2nd line support can be allocated by the IS US Service Delivery Team or Architecture Services. User level Access is initially provided via ITI Architecture Services via the IDM - Active Directory platform provider. Access to services using Active Directory as their main means of authentication and authorisation is determined by the service provider. ITI Architecture (and depending on the service/resource in question - 2nd Line support) provide access to central IS services (the main core of these being provided at account creation time). Owners of services that use AD may have agreements with 3rd party suppliers and may allow access at the Application layers for support and maintenance functions. Architecture Services do not have knowledge of the details of such arrangements.
5.3	Access monitoring	All Active Directory Domain controllers and Windows Servers have extensive security logs, system and application event logs. In addition to there are additional service logs such as local firewall logs on each server, Anti-Virus and Malware utilities both of which log attempted access and potential attacks. The Active directory service can also be configured with various levels of auditing to further increase monitoring of individual objects and services where necessary. Microsoft System Centre Operations Manager is currently deployed which provides for the gathering of such alerts to a central console from where they can be acted upon. There is no active monitoring of user logins. In the event of queries for example over lockouts the logs are checked as part of the resolution process.

5.4	Change control	Active Directory is primarily an 'out the box' product and it's infrastructure is fairly static in nature other than regular security updates which are known to be issued on the second Tuesday of every month (unless there is an exploit which deems an out of band patch). Changes at this level are managed by the ITI-Architecture services Team and in general follow Microsoft guidelines and requirements in order to ensure security and supportability. Where a change may impact or change the service ITI-Architecture will issue a service alert via the IS Service Alerts pages and contact Support teams and other bodies regarding the change, detailing its urgency, the reason for the change and the proposed date. Wherever possible at least one month's notice will be given for production environment changes. It should be noted however during academic term time the service is frozen for major updates unless there is a significant failure or security case.
5.5	Systems clock synchronisation	The Active Directory service's clock is synchronised with the University NTP time server on Cancer.ucs.ed.ac.uk
5.6	Network management	It should be noted that the majority of network management for standard use is via the University's Networking Services. Additional configurations maintained by ITI Architecture within the Active Directory Service are known as IP Subnet based sites. These are a list of locations, and networks forming the network topology as relevant to Active directory. Currently we have two sites defined although this can vary. One is 'UoE Central' which covers the central EDLAN locations and the other is 'Roslin' which is defined as a remote site due to its location and connectivity. Local Firewall Rules and Group Policy based application of these rules to service servers. In addition to the Central Firewall operated by Network Services it is our current policy (unless exclusion can be justified) for ITI Architecture to implement Windows firewall rules (the local OS firewall) using group policy to ensure unnecessary ports are closed and attempted unauthorised port connections logged.
5.7	Business continuity	The Active Directory service is part of the core user experience for staff and student of the University; because of this, a high degree of redundancy and replication is employed to ensure service availability. This includes multiple Domain Controllers split across three sites, a mix of both physical and virtual machines, daily backups of the directory service from multiple sources allowing recovery from total failure, and additional backups capable of granular restore of objects, user and groups. In a disaster scenario only one of the domain controllers for each domain is required to operate the service, however performance would be severely degraded at this level of failure, but it would allow services to function and users to use their workstations until further Domain controllers could be re-provisioned (4-8 hours). Long term Active Directory is a key product of Microsoft and the market leader in the corporate environment. Microsoft continue to integrate Active directory into each of their releases of the operating system and make additions and improvements with each release.
5.8	Security Control	See Network Management.

6. Third Party

[Third parties may be involved as the source provider of the system, or other external organisations and may also be involved in activities related to data held by the system and owned by the System Owner. This section is to draw attention to aspects of managing the system related to involvement by third parties.]

6.1	Outsourcing	None
6.2	Contracts and Agreements	Microsoft Premier Support Contract taken out directly with Microsoft. This is renewed annually from 1st of August. Provides technical support for the Windows Active Directory, Windows Server Operating System and associated Microsoft Windows Server products we have installed including SQL and IIS. The contract consists of 90 hours Support Assistance and 90 hours Problem resolution support. Calls are raised based on severity levels that will provide access to a Microsoft Engineer who will assist with problem resolution. Severity 1 - Catastrophic business impact. 1 hour or less response from call being submitted. Continuous effort 24x7 Severity A - Critical business impact. 1 hour or less response from call being submitted. Continuous effort 24x7 Severity B - Moderate business impact. 2 hour or less response from call being submitted. Effort during business hours 8am-6pm Mon-Fri Severity C - Minimum Business Impact 4 hour or less response from call being submitted. Effort during business hours 8am-6pm Mon-Fri Further details of contract provided in paper format. Held with Architecture Services ITI Division. Microsoft employees do not have on-going access to our Active Directory. A support engineer would be provided access if required to trouble-shoot an issue on the day and then that access would be removed. In the event of Microsoft accessing our systems to provide technical assistance the Premier Support Contract includes a non-disclosure agreement in respect of University data.
6.3	Compliance with the university security policy	Architecture Services Team facility manage file servers on behalf of other Divisions within Information Services at the hardware and operating system layers. Owners of services that use AD may have agreements with 3rd party suppliers and may allow access at the Application layers for support and maintenance functions. Architecture Services do not have knowledge of the details of such arrangements.

6.4	Personal data	In the exceptional circumstances where transfer of data to external organisations takes place this will be done in accordance with University guidance and carried out using secure a secure, encrypted medium in line with current professionally accepted encryption techniques.