

Technical Controls to support the Information Security Policy & Processes

Technical Control	Information Security Policy Ref.	Description
Access controls for System Administrators	To assist IT Professionals across the University	A separate set of credentials from the domain credentials are used to authenticate and authorise users with system administrator roles with higher privilege rights than a regular user would have. In general, access to services and resources granted by the system administrator credentials are orthogonal to those granted by the LANCS domain credentials.
Active Directory [™] Security Group based access permissions Access Control Lists (ACLs)	Access to restricted data must be limited to the minimum required to perform the required task	<p>Users are required to enter a university UserID and password combination to gain access to university systems. Web based systems are protected by the same set of credentials via the Co-Sign single sign on system.</p> <p>Authentication is provided by the users UserID and password, however a separate authorisation stage may be provided by applications / end systems which can use Active Directory groups to further grant or revoke access as required. Where possible Active Directory Groups are automatically reconciled with authoritative data sources such as HR and LUSI.</p> <p>ACLs are the technical way that groups of users are granted access to resources. Only authorised members of staff can modify ACLs,</p>
Mobile Phone Profiles	Restricted data must not be downloaded or copied to mobile devices unless the device is capable of appropriately encrypting the information	<p>Mobile Phones that are specified by ISS and setup by a faculty IT team are provided with a profile which specifies security settings including encryption and PIN lock. Data on iPhones (a supported device by ISS) are encrypted by default, whilst the Nokia E5 has encryption enabled during setup.</p> <p>Guidance for staff using their own devices on the use of restricted data is given as part of the Information Security training</p>

Technical Control	Information Security Policy Ref.	Description
Data Segregation via: Virtual LAN PASS (Permissive Access Security System)	Data Custodians need to ensure that data is secured against accidental disclosure and intentional attempts to access their system	<p>Virtual LAN:</p> <p>The campus network is segmented into a number of virtual LANS (VLANS) that, together with routing between them, provide users connected to different VLANs access to servers that host a number of services. A summary of services and ways in which they can be accessed is provided on the ISS Web Site¹</p> <p>PASS:</p> <p>This system provides access control to the University's wired network. Each device connected to the wired network is registered to a user (or a department e.g. for research machines) for which the following information is recorded;</p> <ul style="list-style-type: none"> • The clients' MAC Address • Switch Name and Port • Connection Time • Connection Duration • Bandwidth Usage • IP Address <p>Furthermore, when a user connects to the network, the PASS system makes an informed decision about what level of network access to allow them based on various criteria such as machine status (i.e. whether known to be virus infected user rights and departmental preference for access level.). With this capability users obtain the correct level of access that their computer/device is registered for in all areas in which the PASS system is deployed (currently the campus wired network).</p> <p>MAC addresses can be easily be changed on many devices however the logging provided by PASS allows the location for each authentication to be recorded. Data points in publicly accessible areas on campus have additional protection to limit the access available to devices connected to them.</p>

¹ <http://www.lancs.ac.uk/iss/index/matrix>

Technical Control	Information Security Policy Ref.	Description
Encryption Training and Guidance	Encrypt all restricted or personal data on your computer; laptop; mobile phone; CD; DVD; external hard disk, USB stick or other data holding device	Guidance ² is provided to users as part of security awareness training, on the web and in our searchable knowledge portal. ISS Supports and assists with the provision of: <ul style="list-style-type: none"> • Ironkey USB sticks • Integral USB sticks • TrueCrypt encryption software • Document encryption using Office 2007/2010 and Adobe Acrobat Pro
Guidance on other methods of file security	When sending email; copying data onto, for example, CDs, laptops, phones or USB sticks; or when working outside the confines of the University you must secure information appropriately.	Guidance on the password protection (and encryption) of Office Documents is provided in our searchable knowledge portal, and covered on mandatory security training. Departmental security reviews also identify the most appropriate control for scenarios in common use.
University VPN Server RDP Group control Secure Desktop Viewing	When working with restricted information away from the University you must always use a secure mechanism such as VPN or Remote Desktop Access.	ISS provides a VPN sever, providing a PPTP secure tunnel over public IP networks with MSCHAPv2 security for user authentication. Users are required to authenticate using their University ID and Password. RDP access is only allowed once the user has connected via a VPN connection, and only when a user has explicitly been added by the Service Desk to use the RDP service. ISS provides, via a 3 rd party, an SSL secured solution for remote desktop viewing. This allows confidential data needing to be seen by others (for example, auditors) to be viewed once over a screen sharing session rather than having to be protected and transmitted.

² <http://www.lancs.ac.uk/iss/security/encryptionoptions/>

Technical Control	Information Security Policy Ref.	Description
Active Directory™ Password Policy	Passwords	<p>The password policy is described to users at https://www.lancs.ac.uk/iss/password/change/</p> <p>A single policy is applied to all usernames:</p> <ul style="list-style-type: none"> • Password history: 10 passwords are remembered • Maximum password age: 425 days • Minimum password age: 1 day • Minimum password length: 6 characters • Password must meet complexity requirements: disabled (but see below) • Account lockout duration: 30 minutes • Account lockout threshold: 10 invalid logon attempts • Reset account lockout counter after: 30 minutes <p>It is felt that the account lockout policy provides considerable protection against a brute force attack, and this allows us to relax the password complexity requirement (which is well-known for making passwords difficult to remember, as described at http://xkcd.com/936/). Obviously weak passwords are rejected by a custom password change filter, which rejects passwords on a “blacklist”. The blacklist currently consists of the “top 1000” passwords (derived from analysis of some password database disclosures [link to password list source required – Steve B should have this]). This list of globally popular passwords has been supplemented with some additions for locally popular passwords (e.g. “Lancaster”, “Liverpool”).</p> <p>The maximum password age setting is higher than many places recommend however is high to discourage the use of incremental passwords such as P@ssw0rd followed by P@ssw0rd2011 and then P@ssw0rdFeb2011 etc.</p>
ISS Group Policy for ISS Managed PCs	Make sure your PC has acceptable anti-virus software installed, keeps its definitions up-to-date and runs a scan at least once a week.	ISS Managed PCs have a mandatory deployment of Symantec Endpoint Protection, whose definitions are kept up to date by a central update server. The software is also provided to staff for use on their personal machines.
ISS Group Policy for ISS Managed PCs ISS Domain Policy for Windows Update	Keep your computer and your web browser up-to-date.	<p>Web browser software updates for non-Microsoft browsers are provided at regular intervals, for ISS Managed PCs via Group Policy deployment.</p> <p>Any Domain joined computer receives Windows Updates for the Microsoft™ Operating Systems via the Windows Software Update Services (WSUS) system.</p>