ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-ISP-014-Secure Working Policy

Owner:	Adrian Hollister
Author:	Paul Ferrier
Date:	26/06/2015
Document Security Level:	**PUBLIC**
Document Version:	2.00
Document Ref:	EA-ISP-014
Document Link:	<URL>
Review Date:	June 2016

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.9	PF	Enterprise Security Architect	Initial version drafted	27/03/2014			
0.91	PF	ESA	Transferred to new document format	12/02/2015			
1.00	PW, AH, GB, CD, PF	IT Director, HoS, EA	Approved policy as Mobile Computing Policy	13/03/2015	Paul Westmore	IT Director	13/03/2015 12:15
1.01	PF	ESA	Converged Remote working and mobile computing policies	11/04/2015			
2.00	PF, CD, PW, DM	ESA, EA, IT Director, Operations Manager	Approved Secure Working Policy	26/06/2015 14:55	Paul Westmore	IT Director	26/06/2015 13:30

EA-ISP-014-Secure Working Policy

Introduction

This policy forms part of the University's Information Security Policy Set and should be read in conjunction with the Information Security Policy (EA-ISP-001), Data Classification Policy (EIM-POL-001) and Use of Computers Policy (EA-ISP-009), Mobile Computing Guidelines (SEC-GDL-006[1]) among other supporting documentation.

Irrespective of where our customers, staff or partners choose to work (including but not limited to, on University property, at home or a temporary or permanent non-University location), access to appropriate resources to perform their duties must be granted if the user and their device can meet or surpass a minimum set of criteria on connection to the University's network; this must be to protect the information assets that are being accessed or manipulated.

There are increased security concerns when work is performed outside of the University's protected environment, as the computers, or user accounts will have the same level of access as on premise users but potentially without the protection provided by office walls, locked doors or network controls.

It is not only security concerns that need to be considered, there are also implications to the legal obligations of health and safety to be adhered to that is outside the scope of this policy.

Please refer to the appendix for further explanation of the points below.

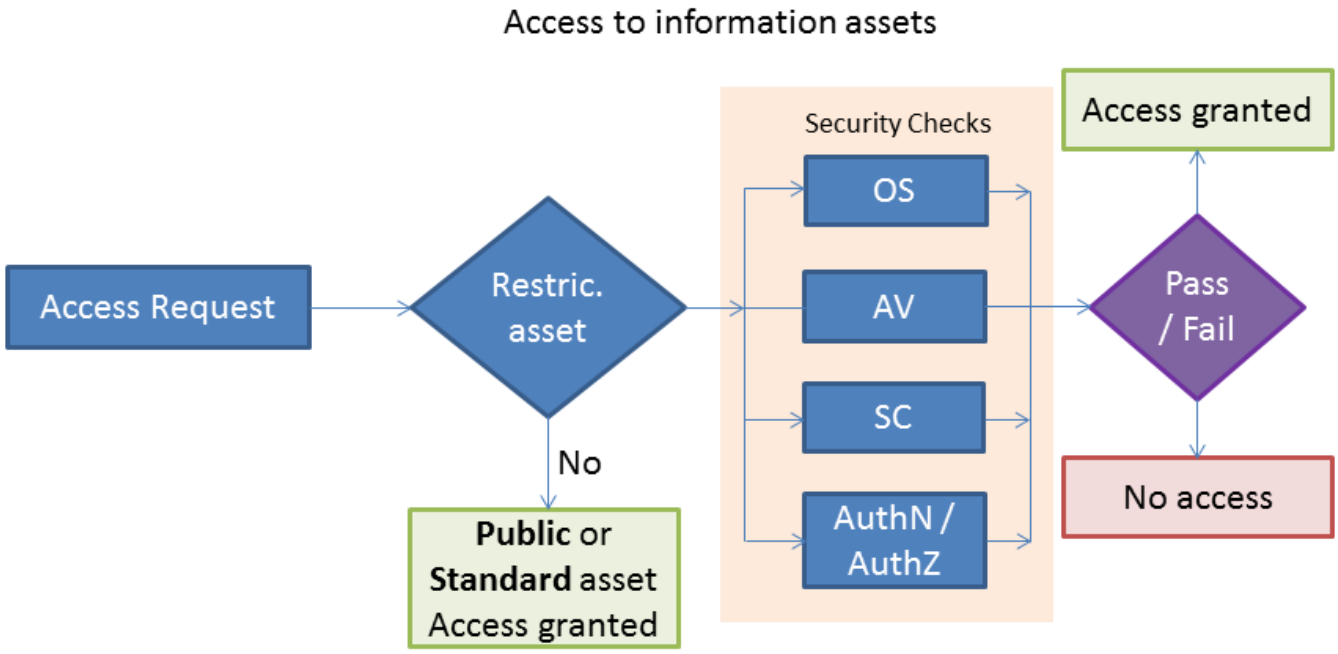
1. Definitions

Anti-malware software	is software that enables interrogation of a computers files, folders and attachments when they are accessed, or when triggered periodically to assess the health of the device, this includes, but is not limited to viruses. Malicious software may impact the legitimate working of the device and potentially leak account credentials or sensitive information without the users knowledge.
Computers	in this policy are presented as a device capable of creating, storing or transmitting information to another computer or device.
Distance learning	is undertaking a form of study where the participants are not required to be situated on the main campus for the core of their teaching and support time.
Mobile working	is working from a non-fixed location, for example, travelling between the office and home or fixed locations.
Remote working	is working from a fixed location, for example, working from home or working from temporary accommodation.
Secure connection	ensures that information in transit between a source and target device is encrypted. This prevents, or makes it significantly harder for disclosure of information to any device listening in to communications.

2. Information access security challenges

2.1 Access to information assets must be prevented for unauthorised users as well as devices that do not offer sufficient assurances surrounding the protection that they offer.

[1] SEC-GDL-006 - Mobile Computing Guidelines



2.1.1 By default, no access is provided to resources classified as **restricted**, in the future if the device passes a series of challenges then access may be afforded[2], these security checks are detailed below:

Patched and Supported Operating System (**OS**)[3]	Any device that is communicating with the University network must have an operating system that is supported by its manufacturer and patched to an appropriate level, the device will be quarantined and access to **restricted** and/or potentially **standard** information may not be possible if this is not the case.
	Working with an up to date Operating System will not only protect the device accessing the information, it will also protect the wider network and its connected resources.
Anti-malware (**AV**) software	Any connection to a University network provides a point of ingress and egress for malicious software to traverse, propagate and could cause widespread problems. When it is possible to interrogate the basic software on a computer this should be encouraged. Any computer that does not have anti-malware software installed or is not up to date with its virus definitions will be quarantined and access to **restricted** and/or potentially **standard** information may not be possible.
	Working and up to date anti-malware will not only protect the device accessing the information, it will also protect the wider network and its connected resources.
Secured network connection (**SC**)	Any connection to an *unsecured wireless network* (for example, the withPlymouth guest network, or a mobile internet hotspot provided in a café) will afford limited access to resources.
	A secured network connection may be required to access certain informational assets (for example, via a secure Virtual Private Network (VPN)) ensuring encryption of communications between the source device and destination service.

[2] Unless specifically stipulated as part of a data sharing or research contract.
[3] A list of supported Operating Systems is available on the Enterprise Architecture Repository

Authentication (**AuthN**) and Authorisation (**AuthZ**)	Any user account trying to connect to **restricted** and/or potentially **standard** information must be validated against an authoritative source for authentication and authorisation to access the relevant information.
	Both authentication and authorisation are required for multiple services that afford access to information, including the secure VPN service itself.

2.2 Staff members who will not be working on the main campus, for example, a change in personal circumstances that require remote working for a period of time, must be authorised to do so by their line manager. Where pertinent, a risk assessment based on the criticality of the information assets to be used and the appropriateness of the proposed remote working location should be carried out.

3. Legislation for working

3.1 Employees who will be doing part or all of their work wherever they are have legal responsibilities that pertain to their location of work, this includes:

- Data Protection Act (1998)
- Health and Safety at Work Act (1974)
- Working Time Regulations (1998)
- Display Screen Equipment Regulations (1992) (amended by the Health and Safety (Miscellaneous Amendments) Regulation 2002)
- Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) (1995)
- Employment Act (2002)

3.2 For any member of staff, irrespective of where they are working if you are not well enough to undertake your normal working duties, this must be declared further information about this requirement can be found on the Human Resources Community Page[4].

4. Environmental considerations

4.1 All members of staff who consume, manipulate or create **restricted** (including, but not limited to commercially sensitive) information must be mindful of discussing these materials in inappropriate locations, for example, on public transport or in a busy coffee shop etc.
Eavesdropping or targeted questioning by interested parties can lead to information disclosure that could result in a breach of contract, financial penalties and damage to any data sharing agreements.

4.2 No **restricted** data on paper shall be left on desks overnight, it must be kept securely in lockable cabinets.

4.3 All users should seek to minimise the production and retention of paper copies of any **restricted** documents. Copies that are no longer required must be destroyed using a cross-cut shredder or placed into confidential waste bags.

4.4 When staff are connecting to services containing restricted information from potentially insecure networks (such as public, hotel or conference free wifi or from home (especially if no security settings have been changed) wireless access points) a secure remote connection[5] must be used.

5. Reporting losses

5.1 All members of the University have a duty to report the loss, suspected loss, unauthorised disclosure or suspected unauthorised disclosure of any information asset through the Enterprise Security Architect (esa@plymouth.ac.uk) or the University's Data Protection Officer (dpo@plymouth.ac.uk).

[4] Human Resources – Sickness and Absence forms and information
[5] Secure Remote Connection documentation for Mac computers or Windows computers

Appendix

2. Information access security challenges

Explanatory Notes

Services, systems and their underlying data can only remain protected if a) they are not used or b) when the computer accessing them can be assured that there is no malicious software on the device awaiting a connection to start collecting, interrogating or exfiltrating data and building knowledge surrounding the inner workings of the service in question. It is understood that option a will almost never occur, as it identifies software that is not needed by the business for general operation and therefore should be removed.

There will always be a need for certain users to be able to complete sensitive or restricted work outside of normal working hours, this however increases the information security risks associated with the work though. Working long hours can introduce inaccuracies in data or a target audience for a communication or document to be passed to; as such additional manual checking must be performed before clicking the button to disseminate this information.

Challenges for someone not working in a permanent fixed location include, but are not limited to:

- The organisation's information assets being stored and accessed from outside the organisation's security perimeter in a location where secure physical and procedural control of information and information systems is unlikely to be the norm;
- The organisation's information assets being accessed in a location shared with non-members of the organisation who may be able to gain unauthorised access to them;
- The possibility that the only copy of an information asset may be held in a remote location whose security cannot be controlled.

3. Legislation for working

Explanatory Notes

The legal responsibilities of the employer in the workplace apply equally to the home working environment. Legislation applicable includes:

Data Protection Act (1998): concerns the processing and storage of personal information, irrespective of where this is carried out. Is the data secured against theft and from viewing by family members and visitors?

Health and Safety at Work Act (1974): ensures the welfare, health and safety of employees wherever they work. Under section 2(4) of the Act safety representatives, appointed by a recognised Trade Union, can represent home workers in any consultations with employers concerning health and safety and welfare matters.

Working Time Regulations (1998): stipulate that, unless opted out of, workers should work no more than 48 hours per week. They also provide directives on breaks taken, and paid annual leave.

Display Screen Equipment Regulations (1992) (amended by the Health and Safety (Miscellaneous Amendments) Regulations 2002): anyone, including remote workers, who uses computers on a regular basis (i.e. for a third or more of their working time for a continuous period of one month), is entitled to an eye test paid for by their employer.

Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) 1995: employers have a duty to report and record work-related accidents, injuries and other occurrences arising from work-related activities, including home working.

Employment Act (2002): an employer may reject an application to commence remote working if the desired working pattern cannot be accommodated by the needs of the business.

This list is not exhaustive.