ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-ISP-014 Secure Working Policy

Owner:	Nick Sharratt
Author:	Paul Ferrier
Date:	08/03/2018
Document Security Level:	**PUBLIC**
Document Version:	2.10
Document Ref:	EA-ISP-014
Document Link:	
Review Date:	March 2019

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
2.10	PW, GB, NS, PF	IT Director, HoSM, 2 x ESA	Update ahead of review	06/03/2018	Paul Westmore	IT Director	06/03/2018 17:20

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), Information Security 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.

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. Legislation for working

2.1 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)
- General Data Protection Regulation (2018)
- Health and Safety at Work Act (1974)

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

- 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)

2.2 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[2].

3. Environmental considerations

3.1 All members of staff who consume, manipulate or create **confidential** or **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.

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

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

3.4 When staff are connecting to services containing **confidential** or **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[3] must be used.

4. Reporting losses

4.1 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 Information Security team (infosecurity@plymouth.ac.uk) or the University's Data Protection Specialist (dpo@plymouth.ac.uk).

[2] Human Resources – Sickness and Absence forms and information

[3] Secure Remote Connection documentation for computers