St George's, University of London
Legacy IT Hardware & Software Security Policy

1. Introduction

Technology becomes legacy because of any or all of the following points.

1.1 The technology now is:

- considered an end-of-life product
- out of support from the supplier or manufacturer
- impossible to update
- no longer cost-effective
- now considered to be above the acceptable risk threshold

2. Policy

2.1 In General, the use of legacy hardware and software (that is products for which the vendor no longer provides support) shall be minimized and, where unavoidable, plans shall be made to move to supported products as soon as possible.

2.2 Where legacy products need to remain in operation the information asset owner shall regularly consult with the IT Department to agree timely controls to be implemented to minimise risks that may occur from continuing usage (including ongoing monitoring effectiveness of implemented controls).

2.3 Where there is no immediate upgrade path, SGUL IT shall isolate systems that register a High or Medium score on the Nessus security scanner.

2.4 This isolation will be total, in that systems that are end of life and unsupported will not be able to access the SGUL network or internet, nor shall they be accessible by SGUL devices.

2.5 This will be achieved either by physical disconnection from the network, or where an entire "lab" or "suite" continues to require network connectivity, they shall be moved to an isolated VLAN.

2.6 Where a device is running a non-critical application on an otherwise supported platform, and that application registers a High or Medium score on the Nessus security scanner, the application will be removed.

2.7 Examples of this are end of life versions of Office, Adobe products, Flash, etc.

3. Supporting Polices

- Patch management policy
- Secure configuration policy