Device and Network Security Policy

Introduction

This policy provides a framework to ensure security requirements of services offered by and data stored, processed and transmitted by devices are identified and managed. It contains significant elements of the ITS Device Security Policy (Draft) but extends some definitions and requirements for the School of Information Technology and Computer Science (SITACS).

Definitions

Device is Hardware and software or firmware that form an information technology apparatus and offers a service or services to users and may store, transmit and process data.

User is a person who uses a service offered by a device

School is the School of Information Technology and Computer Science

Scope

This policy applies to any device owned by, under the control of or connected to the University network that satisfies any of the following criteria:

The device stores, processes or transmits data that has requirements with respect to confidentiality, integrity or accessibility which if breached affects the business of the University or the privacy of a user or users other than the single primary user of the device.

The device offers a service or services

An officer of the School responsible for the device decides to apply this policy for reasons other than the criteria above

Purpose

The purposes of this policy are:

Assigning responsibility for the security of devices.

Identification and consideration of security issues relating to the services devices offer and to data stored, processed or transmitted by these devices.

Identification of security requirements of devices and avoidance of conflicting requirements

Planning, implementation and management of measures to meet identified security requirements of devices

Provision of minimum security requirements that must be met or exceeded by the processes derived form this policy for devices.

Identification of Security Issues

Performing regular risk assessments will identify security issues relating to devices that fall within the scope of this policy. Threats posed to services offered by the device, data stored, manipulated or transmitted and to other devices on the network shall be identified.

Meeting Security Requirements

Measures necessary for meeting the identified requirements shall be chosen with consideration given to the implementation and ongoing management and maintenance of these measures.

Base Security Level

The following minimum set of security requirements will be met or exceeded by any device falling within the scope of this policy:

Least access

The device offers only services to meet specific requirements of identified users

The services offered by the device are accessible only to the identified users

Least privilege

Users of the device have access to only the services and data which is required to meet their needs

Administrative access to the device is limited to a small number of identified individual users

Disaster Recovery

Measures should be implemented to recover the services offered and data stored by the device within an acceptable period of time* following a disaster.

Reliability and Integrity

Measures are implemented to ensure the ongoing reliability of services offered and integrity of data stored on the device.

Auditing and Logging

Audit trails and logs of events are kept which assist in recognising and investigating breaches of security requirements of the device.

Physical Security

Measures are implemented to mitigate significant risks to the hardware component of the device.

Example Devices

Devices that fall under the requirements of this policy include:

- USB Memory Device
- Detachable Hard Disk Drive