SECURE COMPUTER AND INTERNET RESOURCES IN PRISONS
Ron Fabre
Cyber IT Solutions Pty Ltd
October 2011

This paper provides an overview on the current state-of-play of secure computer resources and Internet access available to correctional facilities for the purposes of prisoner education, rehabilitation and recreation.

Introduction
The intended audience of this paper is education policy makers and executive directors of correctional facilities. This paper offers a solution to the technical and logistical challenges of providing prisoners with managed secure access to valuable computer resources within prisons.

Many prisons today provide computer facilities for use by prisoners to facilitate prisoner education and rehabilitation, the preparation for legal proceedings, and to reduce boredom.

Security is the primary concern when providing prisoners with any access to electronic devices. Prisoners must not be able to communicate clandestinely or hide any physical or electronic contraband from custodial staff.

Objectives
There are a number of business drivers for making computer resources available to prisoners in our correctional facilities.

Academic Education
Basic education in numeracy and literacy must be provided to all prisoners, upon which all further adult education is reliant.

Human Rights
Many jurisdictions are beginning to recognise in law that Internet access is a fundamental right on a par with freedom of expression (ref page 5).
Work-place Skills

The majority of occupations involve interaction with a keyboard and screen. Prisoners lacking these work-place skills will be implicitly restricted to only manual labour. Vocational education and training is a major influence in the reduction of recidivism.

Legal Preparation

Prisoners facing legal proceedings must be able to prepare for their defence and collaborate with their legal representatives. This often requires substantial time reviewing electronic evidence and editing legal documents.

Entertainment

Prisoners who have access to entertainment are less likely to be susceptible to boredom and its consequences. Indeed many correctional facilities allow prisoners access to entertainment devices such as games consoles, televisions, stereos, and video players.

Challenges

The introduction into prisons of off-the-shelf computers brings with it a number of security and safety risks. These risks must be adequately responded to, otherwise the computer resources and their educational benefits will likely be removed from the facility by prison management.

Contraband

It is common for custodial staff to spend multiple hours on a regular basis auditing devices for physical and electronic contraband, an error prone and labourious process.

Optical media (DVDs) and USB storage devices ('thumb-drives') are a valuable and tradeable item, and can contain electronic contraband.
**Illicit Communication**

Prisoners will try to communicate clandestinely, sometimes via written notes in physical 'drop-boxes' and, if given the opportunity, via electronic documents. Successful exploitation of these opportunities and a lack of appropriate monitoring can leave evidence of planned crimes undetected until after the crime is committed, or expose prisoners and third parties to serious risk of harm due to confidential data being discovered by other prisoners (ref page 5).

**Management Cost**

The implementation of off-the-shelf computer equipment and software attracts a substantial management overhead. Each computer must be regularly audited for contraband and have software reinstalled, and this must be done within physical proximity of the device.

**Physical Safety**

Off-the-shelf computers normally include cables of more than 150mm in length, posing a safety hazard for prisoners who can use them for self harm or as weapons against other prisoners.

**Opportunities**

Any computer solution made available to prisoners must be designed with multiple layers of security, while ensuring that the overall solution provides the necessary educational experience.

**Monitoring**

Custodial staff must have full visibility of prisoners’ system usage. Staff should be able to clandestinely monitor active/current usage, and review details of previous activity. All usage history and logs must be stored securely so that prisoners and staff can not tamper with evidence.

Unauthorized attempts to gain access to any feature must trigger appropriate alerts to custodial staff so that timely action can be taken.
Filtering

All computer-based services available to prisoners should be filtered to ensure that only specific prisoners or groups of prisoners can utilise each service.

Prisoners' access to web and email must be suitably restricted such that they can access only approved URLs and communicate only with approved email addressees, thereby denying their ability to communicate clandestinely with each other or with outside entities.

Electronic fingerprinting of optical media must be employed. Each disc should be assigned to a subset of prisoners (or a single prisoner) so that the disc can not be traded. This will also result in prisoners being unable to utilise unauthorised media smuggled into the facility.

Security - Physical and Electronic

Prisoners do not require access to USB storage devices ('thumb-drives') or USB communication devices (3G modems, WiFi, etc), however as these devices will inevitably be smuggled in to the facility then such devices must be blocked at the system level. Custodial staff must be alerted when a prisoner attempts to make use of these devices.

It is important to ensure that all computer cables are no longer than 12''/30cm, thereby reducing the opportunity for prisoners using them for self-harm or as weapons.

All users' data must be stored securely on non-removable media, and accessible only by the prisoner and appropriate custodial staff. Staff must be able to review prisoners' data clandestinely and without visiting the secure area of the facility.

Curfews

Custodial staff must be provided the flexibility to impose curfews on the use of computers and of individual services. This will reduce the hours during which monitoring of computer activity is required, and will provide staff with a valuable tool for prisoner discipline.

Management

Access to the management facilities must be restricted to only staff computers, and all such traffic must be SSL encrypted.
References
