UNIVERSITY of TASMANIA

ICT Physical Security Procedure

UNDER REVIEW

Related Policy	ICT Security Policy
Responsible Officer	Chief Information Officer
Approved by	Chief Information Officer
Approved and commenced	August, 2014
Review by	August, 2017
Responsible Organisational Unit	Information Technology Services

CONTENTS

1 Objective

This document provides minimum standards for implementing physical control measures to protect ICT Facilities and Infrastructure at the University of Tasmania.

2 Scope

All data centres, node rooms, and computing and communications areas controlled by IT Resources

3 Procedure

Step	Details	Responsibility
1.	Physical access controls around computing spaces are to be applied in a manner that reflects the business value of ICT Services hosted in a space, the value of data stored in a space, and the criticality of ICT Facilities and Infrastructure housed in a space.	ICT Security Manager Chief Information Officer
2.	The University of Tasmania's critical computing spaces will employ the following controls: • Barrier; • Combination electronic and physical lock; • Auditable access (via proxy card or key code entry); • Video surveillance; and • Monitored alarms: o Motion sensing o Forced entry o Fire (VESDA) o Temperature o Power status. Authority to access a critical computing location, or barrier areas surrounding the location, may only be given by the Chief Information Officer, or a nominated representative.	ICT Security Manager Chief Information Officer
3.	Computing spaces that are identified as important, but not critical, will employ the following controls: • Barrier; • Combination electronic and physical lock; • Auditable access (via proxy card or key code entry); and • Monitored alarms: o Forced entry o Fire o Temperature. Authority to access a non-critical computing location may only be given by the Chief Information Officer, or a nominated representative.	ICT Security Manager Chief Information Officer

4.	ICT centres, such as computer laboratories, switch locations, and other remote locations where ICT assets are housed must employ physical access controls such as electronic or physical locks. Controls must be in place to: • reduce unauthorised access to assets; • reduce the threat of asset theft. The appropriate level of physical security controls will be determined by risk assessment of the space, and the criticality of the ICT Facilities and Infrastructure housed in the location. The risk assessment must consider what ICT Facilities and Infrastructure can be accessed (including electronically) from the site being assessed.	ICT Officer ICT Security Manager Chief Information Officer
5.	All cabling must be managed as per the Information Technology Services Telecommunications Cabling Specification and Standard	ICT Officer ICT Security Manager

4 Definitions and Acronyms

ICT	Information and Communication Technologies
ICT Facilities	All computers, terminals, telephones, end host devices, licences, centrally managed data, computing laboratories, video conference rooms, and software owned or leased by the University.
ICT Infrastructure	All electronic communication devices, networks, data storage, hardware, and network connections to external resources such as AARNet and the Internet.
ICT Security Manager	The ITS appointed representative responsible for ICT security.
ICT Services	All systems supporting interaction, information provision, information storage, or communications provision and the ICT Facilities on which they operate.
University	The University of Tasmania

5 Supporting Documentation

- ICT Security Policy

6 Versioning

Former Version	ICT Physical Security Procedure, approved May, 2011; reviewed May, 2014
Current Version	ICT Physical Security Procedure; minor amendments to update terms/references; approved by Responsible Officer, Chief Information Officer, August, 2014.