cloudtronics

Physical and Environmental Security (PES) Policy

Version 1.0

February 2019

TABLE OF CONTENTS

DOCUMENT CONTROL

This is a controlled document.

All changes must be authorised by the document owner and tracked below.

DOCUMENT OWNER

Owner:	Robert Nathan
Phone:	1800 876 642
Email:	admin@cloudtronics.com.au

DOCUMENT HISTORY

Version	Date	Summary of changes
0.1	7 February 2019	Robert Nathan – Initial version.
1.0	8 February 2019	Approved by Robert Nathan.

INTRODUCTION

OBJECTIVE

This objective of the *Physical and Environmental Security (PES) Policy* is to prevent unauthorised physical access, damage and interference to the organization's premises, information and equipment.

SCOPE

This policy applies organisation-wide including:

- information created or received by the company in hardcopy or electronic form
- systems (e.g. hardware & software) used to store, process or transmit company information
- people accessing company information (employees, contractors and external parties)
- physical assets used to protect company information
- suppliers that store, process or transmit company information on behalf of the company

GENERAL RESPONSIBILITIES

Role	General responsibilities
Executive	• Approve the Information Security Management Framework (ISMF) policy and monitor performance
ISGC	• Approve this and other policies, standards and procedures
Managers	• Apply policies and associated procedures on a risk-managed basis
All	• Conform with company policies such as this and associated procedures • Report suspected or actual deviations to management: (e.g. via security@cloudtronics.com.au)

Further specific responsibilities are assigned in each policy.

GLOSSARY OF TERMS

Refer to the glossary of terms as required.

STATEMENTS

The *Physical and Environmental Security (PES) Policy* addresses the following topics:

- Site selection
- Perimeter controls
- Entry controls
- Area controls
- Cabling
- Equipment

Other topics are addressed in complimentary policies, standards, guidelines and procedures.

SITE SELECTION

The *Executive*:

Ref	Statement	
PES-1	Selects sites for computer processing facilities with consideration to: 1. environmental threats (such as fire, flood and hurricanes), and 2. physical security threats (e.g. crime rate, acts of terrorism)	

PERIMETER CONTROLS

The *Physical Security Manager*:

Ref	Statement	
PES-2	Implements effective perimeter controls to avoid unauthorised access to company assets including: • fencing and/or walls • lighting • video surveillance • concrete “slab-to-slab” construction Note: Concrete “slab-to-slab” construction or alternative treatments such as welded steel mesh/grills are defined in the Australian Government Physical security management guidelines as follows: https://www.protectivesecurity.gov.au/physicalsecurity/Pages/SecurityZonesAndRiskMitigationControlMeasuresGuidelines.aspx	

ENTRY CONTROLS

The *Physical Security Manager*:

Ref	Statement	
PES-3	Implements effective entry controls to control staff, contractor and guest access to company assets including: • managed reception area • card access control system or lock/key • guest registration and identification procedures Note: Effective entry controls are described in the Australian Government Physical security management guidelines as follows: https://www.protectivesecurity.gov.au/physicalsecurity/Pages/SecurityZonesAndRiskMitigationControlMeasuresGuidelines.aspx	

AREA CONTROLS

The *Physical Security Manager*:

Ref	Statement	
PES-4	Secures areas where assets are stored unattended or unencrypted including: • security alarm system incorporating intrusion monitoring sensors • security containers for the storage of paper and other assets Note: Effective area controls are described in the Australian Government Physical security management guidelines as follows: https://www.protectivesecurity.gov.au/physicalsecurity/Pages/SecurityZonesAndRiskMitigationControlMeasuresGuidelines.aspx Note: In open planned offices, it is recommended that adequate meeting rooms exist with acoustic treatment to allow for sensitive conversations.	

EQUIPMENT

The *IT Manager*:

Ref	Statement	
PES-5	Stores assets securely such as in a locked cabinet in order to prevent theft, unauthorised modification or destruction.	

ENVIRONMENTAL CONTROLS

The *IT Manager*:

Ref	Statement	
PES-6	Ensures suitable environmental controls used to provide power and cooling to equipment.	

PES-7	Ensures all systems with a High availability classification are protected with redundant power (i.e. dual power feeds, UPS and generators).	
PES-8	Ensures all systems with a High availability classification are equipped with temperature detection and are configured to automatically shutdown when defined thresholds are exceeded to avoid damage. Note: Temperature controls can be configured within the hardware of individual systems, with auxiliary components or on masse.	
PES-9	Ensures all areas housing systems with a High availability classification are equipped with fire suppression. Note: Water (sprinklers) as a fire suppression mechanism should be avoided and approved gas agent (e.g. FM200) used instead. CO2 fire extinguishers may also be an option depending on local fire codes and scale of facilities.	

CABLING

The *IT Manager*:

Ref	Statement	
PES-10	Minimises the amount of cabling through which unencrypted communications pass.	
PES-11	Physically secures cabling within an access controlled or tamper evident barrier where plaintext communications outside the physically secure perimeter.	
PES-12	Ensures cabling carrying any unencrypted communications uses dedicated conduit or reticulation system, i.e. separate from public networks.	***ISM***
PES-13	Enables cabling associated with unencrypted High classified information is blue where possible and a different colour is used for external networks.	***ISM***
PES-14	Labels cables and maintain patch plan(s) / cable register(s).	***ISM***
PES-15	Inspects cabling for inconsistencies with the patch plan(s) / cable register(s) at least annually.	***ISM*** ⏰

ASSURANCE

The *Physical Security Manager*:

Ref	Statement	
PES-16	Arranges to receive advice from a SCEC Zone Consultant if implementing new or upgrading an existing perimeter, secure area, or entry controls that are used to protect any Highly confidential information.	***ISM***