cloudtronics

Network Security (NETS) 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 *Network Security (NETS) Policy* is to protect information in transit over computer networks.

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 *Network Security (NETS) Policy* addresses the following topics:

- Network segregation
- Internet gateways
- Wireless networks
- Voice and videoconferencing networks
- Network encryption
- Network availability

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

NETWORK SEGREGATION

The *IT Manager*:

Ref	Statement	
NETS-1	Segments critical systems with network controls. Note: Critical systems are any assets with a High availability classification. Note: Network controls includes firewall rules.	
NETS-2	Uses logical network segregation (such as VLANs) and jump servers to permit access administrator zones. Note: Jumphosts act as focal points within the administration environment and allow for communication restrictions.	***ISM***

NETWORK GATEWAYS

The *IT Manager*:

Ref	Statement	
NETS-3	Segments internal systems from the public networks with gateways. Note: Internal systems are used by staff and contractors only are not accessible to customers, partners or members of the public. Note: Gateways are firewalls.	
NETS-4	Ensures gateways: • are the only communications paths into and out of internal networks • by default, deny all connections into and out of the network • allow only explicitly authorised connections • permit content filtering • are managed via a secure path isolated from all connected networks • provide sufficient logging • provide real-time alerts • include an intrusion detection and prevention system	***ISM***

NETS-5	Ensures gateway inspect traffic at the application layer or are passed to an application aware proxy in a De-Militarised Zone (DMZ). Note: A DMZ sits in between the public internet and internal networks.	
NETS-6	Tests the security measures incorporated into internet gateway at irregular intervals at least quarterly.	***ISM***
NETS-7	Reviews the security architecture of the gateway and firewall rules on internet gateway at least annually.	⏰

WIRELESS NETWORKS

The *IT Manager*:

Ref	**Statement**	
NETS-8	Segments wireless from internet networks with gateways.	
NETS-9	Configures the wireless network as follows: • Disable administrative interface on wireless access connections • Change the default SSID to something unrelated to the organisation • Ensure the SSID is broadcasted • Enable CCMP	
NETS-10	Enables encryption and authentication using WPA2-Enterprise with EAP-TLS for wireless networks used for business purposes. Note: WPA2-PSK may be used for visitors/guests, personal use or remote access only. Note: Use both device and user certification when configuring authentication.	***ISM***
NETS-11	Uses many lower power wireless access point instead of a small number of high powered wireless access points to prevent the network footprint extending beyond the perimeter of the organisation.	***ISM***

VOICE AND VIDEOCONFERENCING NETWORKS

The *IT Manager*:

Ref	**Statement**	
NETS-12	Segments voice and video networks from internal systems with gateways using a voice and/or video-aware firewall (as appropriate).	
NETS-13	Enables encryption and authentication to protect signalling and data protocols.	***ISM***
NETS-14	Configures voice and video communication as follows: • devices authenticate themselves to the controller upon registration • auto-registration is disabled and only a whitelist of authorised devices are allowed to access the network • unauthorised devices are blocked by default • all unused and prohibited functionality is disabled	***ISM***

NETS-15	Does not connect workstations to video conferencing units or IP phones unless the workstation or the device uses VLANs or similar mechanisms to maintain separation between video conferencing, IP telephony and other data traffic.	***ISM***
NETS-16	Limits the ability of any IP phones or videoconferencing units in lobby and shared areas to access data networks, voicemail and directory services.	***ISM***
NETS-17	Maintains a plan in the event digital networks including voice and video networks are the subject of a Denial of Service (DoS) plan. Note: In low risk environments, this may involve the use of mobile phones. Or in other cases, redirecting numbers or relying on traditional DoS protections.	***ISM***

NETWORK ENCRYPTION

The *IT Manager*:

Ref	Statement	
NETS-18	Encrypts all networks extending beyond the organisation's physical secure perimeter.	
NETS-19	Encrypts all information with a Medium confidentiality rating transiting a public network with at least an ASD Approved Cryptographic Algorithm and Protocol (AACA and AACP). Note: The AACAs and AACPs can be found in the Australian Government Information Security Manual (ISM) as follows: https://www.asd.gov.au/infosec/ism	***ISM***
NETS-20	Encrypts all information with a High (or Protected) confidentiality rating transiting a public network with an encrypted Virtual Private Network (VPN) using Transport Layer Security (TLS) or IPSec.	
NETS-21	Uses an ASD Approved Cryptographic Protocol (AACP) when performing administration of systems (e.g. SSH, TLS or VPN).	

NETWORK AVAILABILITY

The *IT Manager*:

Ref	Statement	
NETS-22	Ensures critical systems have redundant network paths such that any single points of failure are removed.	

NETWORK CONFIGURATION

The *IT Manager*:

Ref	Statement	
NETS-23	Ensures network equipment supports IPv6 but disables IPv6 unless required.	***ISM***

NETS-24	Ensures network equipment is configured to SNMPv3, disables SNMPv1 and SNMPv2, change default community strings and have write access disabled.	***ISM***
NETS-25	Disables unused network ports.	

NETWORK DOCUMENTATION

The *IT Manager*:

Ref	**Statement**	
NETS-26	Maintains network documentation that includes: • high-level network diagram showing all connections into the network • a logical network diagram showing all network devices, critical servers and services • the standard configuration of network devices	***ISM***
NETS-27	Updates network documentation as network architecture and configuration changes are made and include document control (i.e. date last updated), or at least annually.	⏰

NETWORK TESTING

The *IT Manager*:

Ref	**Statement**	
NETS-28	Arranges for network scans to identify authorised and potentially unauthorised devices connected to the network at least quarterly. Note: This may be conducted as host discovery during periodic vulnerability scans.	***ISM*** ⏰