System Acquisition & Development (SAD) 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 *System Acquisition & Development (SAD) Policy* is to ensure that information security is designed and implemented with the development or acquisition of new systems.

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 *System Acquisition & Development (SAD) Policy* addresses the following topics:

- Requirements
- Development environments
- Test data
- Version control
- Code escrow
- Secure code
- Cryptography
- Security testing

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

REQUIREMENTS

The *IT Development and/or Procurement Manager*:

Ref	Statement	
SAD-1	Ensures the business requirements for the development or acquisition of new systems include requirements for security. Note: The requirements should reflect the requirements found in the cyber & information security policies and standards including: • Physical and personnel security (if required) • IT Operations management including vulnerability management • Identity and access management • Network security • Cryptography • Business continuity	
SAD-2	Requires defined security service levels to be agreed with supplier to ensure adequate performance of security controls and security activities. Note: Service levels may include those for: • Timely reporting of security vulnerabilities and incidents • Timely access to services or information • Timely changes to services or information	

DEVELOPMENT ENVIRONMENTS

The *IT Development Manager*:

Ref	Statement

SAD-3	Separates development and test systems (and any other non-production systems) from production systems to avoid disruption. Notes: Virtual separation such as virtual host and VLANs is adequate.	
SAD-4	Ensures new development and modifications of software only take place in the development environment.	
SAD-5	Controls the staging and release of code from one environment to the next in a controlled manner.	

TEST DATA

The *IT Development Manager*:

Ref	Statement	
SAD-6	Ensures development and test systems use only test data (not production data). Notes: To achieve this requirement, test data can rely on artificial data or sanitised copies of production data.	

VERSION CONTROL

The *IT Development Manager*:

Ref	Statement	
SAD-7	Stores developed software in a version control system (e.g. Git).	
SAD-8	Restricts access to the version control system.	

CODE ACCESS

The *IT Development Manager*:

Ref	Statement	
SAD-9	Retains direct access to code in the version control system or indirectly via software escrow arrangements.	

SECURE CODE

The *IT Development Manager*:

Ref	Statement

SAD-10	Requires developers to apply secure coding practices (e.g. OWASP) and consider threat modelling and other secure design techniques. Note: Secure coding practices include: • Input validation • Output encoding • Encryption of sensitive data at rest • Encryption of sensitive data in transit • Hashing of data where integrity is important • Session management • Error handling • Logging	
SAD-11	Requires developers to verify libraries are up-to-date and free from vulnerabilities. Note: Tools such as OWASP Dependency Check and Snyk can help to achieve this objective.	

CRYPTOGRAPHY

The *IT Development Manager*:

Ref	Statement	
SAD-12	Employs cryptographic algorithms and protocols approved by the Australian Signals Directorate (ASD) where performing cryptographic functions such as encryption, hashing and digital signatures. 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	
SAD-13	For passwords, uses strong password specific hashing algorithms in preference to standard hashing algorithms along with unique salts in order to reduce the opportunity for brute force attacks. Note: Strong password specific algorithms include Argon2, PBKDF2 and bcrypt.	

SECURITY TESTING

The *CISO*:

Ref	Statement	
SAD-14	Tests (or arranges for testing of) software for vulnerabilities prior to use in a production environment, after significant change or at least quarterly. Note: This includes application level security testing.