ITSS_21 IT Security Standard – Secure Algorithm List ("SAL")

Version	Approved by	Approval date	Effective date	Next review
1.0	Vice-President, Finance and Operations	10 May 2017	10 May 2017	May 2020

Standard Statement

Purpose	UNSW has established a need for securing business data through the use of cryptography in data encryption, data hashing and data masking. These security controls are prescribed in the *Data Classification Standard, Data Handling Guidelines* and UNSW Security policies and standards This supporting *Secure Algorithm List ("SAL")* Standard has been developed to ensure that UNSW's cryptographic and masking practices are effective and are not prone to evolving security threats, emerging cryptanalysis techniques and/or cryptographic attacks. The SAL is aligned with organisational objectives, Industry best practice guidelines and where possible the objectives defined by the Payment Card Industry Data Security (PCI DSS) Standard.	
Scope	This supporting Standard is applicable to all users and systems that are bound by the UNSW policies and standards	
Are Local Documents on this subject permitted?	☐ Yes, however Local Documents must not breach mandatory requirements in University-wide Codes of Conduct, Policies, Standards and Procedures.	☐ No

Standard

1. Common Encryption Scenarios

The use of cryptography is dictated by UNSW data classification and/or regulatory requirements.

There are two basic types of cryptography: symmetric and asymmetric.

There are three main uses for cryptography:

- **Confidentiality** (data encryption)
- **Integrity** (encrypted checksums over data)
- **Identification** (digital signatures and certificates)

The use of Cryptography is determined by UNSW defined Security Controls, Policies and Procedures commensurate with a systems Data Classification.

Guidance on common scenarios for the use of cryptography are presented in the below table.

Security Classification	Internal Facing UNSW System		External facing UNSW System		Cloud Hosted System	SOE Laptops, SOE Desktops, UNSW provided removable media and portable devices	BYOD Laptops, removable media and portable devices
	Storage	**Transmission**	**Storage**	**Transmission**			
Public	Recommended	Recommended	Recommended	Recommended	Recommended	Not Required	Not Required
Private	Recommended	Recommended	Recommended	Recommended	Recommended	Recommended	Recommended
Sensitive	Encrypt	Encrypt	Encrypt	Encrypt	Encrypt	Encrypt	★Highly Recommended
Highly Sensitive	Encrypt	Encrypt	Encrypt	Encrypt	Encrypt	Encrypt	★Highly Recommended

★ UNSW Policy and BRIDG Data Handling guidelines should be consulted prior to intentionally exposing data classified as '*Sensitive*' or '*Highly Sensitive*'; to unmanaged BYOD endpoints. The use of Threat modelling and Risk assessment practices are strongly encouraged.

📖 **UNSW**

- IT Security Standard - Information Security Risk & Compliance Management - ITSS_17
- IT Security Standard - Bring Your Own Device "BYOD" - ITSS_13

2. Approved Algorithms

The following describes the various Approved Algorithms and caveats of use.

2.1 Approved Asymmetric / Public key Algorithms

When selecting asymmetric cryptographic algorithm, the use of Cryptographic systems MUST be limited to the algorithms specified in the table below. RSA SHOULD be used in preference to Diffie-Hellman. Diffie-Hellman key exchanges MUST NOT be used to establish identity (*Refer to paragraph 3 "Algorithms & Corresponding Key Lengths", "Identity/ Asymmetric Algorithms", page 3*).

Algorithm	Note
Diffie–Hellman (DH)	Used for agreeing on encryption session keys
Digital Signature Algorithm (DSA)	Used for digital signatures
Elliptic Curve Diffie–Hellman (ECDH)	Used for agreeing on encryption session keys
Elliptic Curve Digital Signature Algorithm (ECDSA)	Used for digital signatures
Rivest–Shamir–Adleman (RSA)	Used for digital signatures and passing encryption session keys or similar keys.

2.2 Approved Hashing Algorithms

When selecting a hashing algorithm, the use of Cryptographic systems MUST be limited to the algorithms specified in the table below.

Algorithm	Note
Secure Hashing Algorithm 2 (SHA 2)	

2.3 Approved Symmetric Encryption Algorithms

When selecting a hashing algorithm, the use of Cryptographic systems MUST be limited to the algorithms specified in the table below.

Algorithm	Note
Advanced Encryption Standard (AES)	key lengths of 128, 192 and 256 bits
Blowfish	key lengths of 256+ bits

3. Algorithms & Corresponding Key Lengths

The ciphers listed in the below table are approved for use commensurate with the UNSW Data Classification and Data Handling requirements. It should be noted that a strong preference for stronger ciphers such as AES is indicated.

Security Classification	Type of assurance required				Key Exchange Protocols
	Confidentiality		Integrity	Identity	
	Symmetric Algorithm	Asymmetric Algorithms	Hashing Algorithms	Asymmetric Algorithms	
Public	N/A	N/A	SHA-2 ★	ECDSA-521 ★ DSA-1024+ ★ RSA-1024+ ★	N/A
Private	Blowfish-256+ AES-128+	RSA-1024+	SHA-2	ECDSA-521 DSA-1024+ RSA-1024+	ECDH-384+ DH-1024 (Group 2) DH-2048 RSA-1024+
Sensitive	Blowfish-256+ AES-128+	RSA-2048+	SHA-2 (SHA-256, SHA-384+)	DSA-2048+ RSA-2048+	DH-1024 (Group 2) DH-2048 RSA-2048+
Highly Sensitive	Blowfish-448 AES-256+	RSA-2048+	SHA-2 (SHA-384+)	DSA-2048+ RSA-2048+	RSA-2048+

✪ All new systems MUST NOT use **RC4** or **MD5** regardless of legacy requirements.
★ The **Integrity** of hosted Public data is a Key Reputational concern for UNSW.

4. Cryptographic Communication Security Protocols

4.1 SSL/TLS

The following SHOULD be used:

- TLS v1.1
- TLS v1.2 – preferred if supported.

The following MUST NOT be used:

- SSL version 1
- SSL version 2
- SSL version 3

SSL has been removed as an example of strong cryptography in the PCI DSS, and can no longer be used as a security control after June 30, 2016.

The following SHOULD NOT be used where feasible and MUST NOT be used on any system within the scope of PCI DSS compliance:

- TLS 1.0

4.2 SSH

The following MUST NOT be used:

- SSH version 1

The following SHOULD NOT be used:

- SSH host authentication. Host authentication can be simulated through the use of user-based authorised keys.

SSH MAY use user-based authorised keys instead of password authentication.

4.3 Kerberos and NTLM

NT LAN Manager (NTLM) authentication protocols have known security weaknesses, and are not appropriate where other mechanisms are available.

The following MUST be applied:

- If a platform supports Kerberos, Kerberos mechanisms MUST be used in place of NTLM or other legacy protocols.

- Should an authorized exception exist to accommodate NT LAN Manager (NTLM) authentication, NTLM2 MUST be used in preference to NTLM1.

4.4 LDAP/LDAPS

Where the use of Lightweight Directory Access Protocol (LDAP) is required, it MUST be

- Encrypted and;
- SHOULD use Secure LDAP/LDAP over SSL (LDAPS). The LDAPS Configuration must be limited to TLS as per the SSL/TLS restrictions in paragraph 4.1, page 3.

The following SHOULD not be applied:

- Unencrypted Lightweight Directory Access Protocol (LDAP) SHOULD not be used.
- The use of StartTLS for LDAP SHOULD not be used.

5. ISMS Mapping with Industry Standards

The table below maps the UNSW IT Secure Algorithm List with the security domains of ISO27001:2013 Security Standard and the Principles of Australian Government Information Security Manual.

ISO/IEC 27001:2013	Information Security Manual
10.1 Cryptographic Controls	Cryptography

The following industry standards have been consulted in relation to the advice provided in this UNSW standard.

Payment Card Industry Data Security Standard (PCI DSS) v3.2	US GOVERNMENT FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION (FIPS) PUB 140-2
	Security Requirements for Cryptographic Modules

6. Document Review, Approval & History

This section details the initial review, approval and ongoing revision history of the standard. Post initial review the standard will be presented to the ISSG recommending the formal UNSW policy consultation and approval process commence. A review of this standard will be managed by the Chief Digital Officer on an annual basis.

7. Quality Assurance

This document was designed and created by external and internal consultants in consultation with internal key technical subject matter experts, business and academic stakeholders.

8. Sign Off

Accountabilities	
Responsible Officer	Chief Digital Officer
Contact Officer	ITpolicy@unsw.edu.au
Supporting Information	
Legislative Compliance	Nil
Parent Document (Policy)	IT Security Policy
Supporting Documents	Nil
Related Documents	Data Classification Standard Data Handling Guidelines UNSW Information Security Management System (ISMS) Base Document ITSS_17 IT Security Standard - Information Security Risk & Compliance Management ITSS_13 IT Security Standard - Bring Your Own Device "BYOD"
Superseded Documents	Nil
File Number	2017/12280
Definitions and Acronyms	
No terms have been defined.	

Revision History				
Version	**Approved by**	**Approval date**	**Effective date**	**Sections modified**
1.0	Vice-President, Finance and Operations	10 May 2017	10 May 2017	This is a new document