Cryptographic Policy

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins
Chief Information Security Officer

Document History

Version	Author	Comments	Date
V 0.1	Andrew Clarke	Initial Draft	03/04/2017
V0.2	Andrew Clarke	PWG Technical amendments and exceptions	06/04/2017
V0.3	Andrew Clarke	Amendments from CISA – conditionally approved	21/04/2017
V 0.4	Andrew Clarke	Amend Mick Jenkins role to CISO; Change from demanding encryption on all PII communications to external only;	17/08/2017
V 1.0	Andrew Clarke	Approved InfoSub Committee	26/01/2018
V 1.1	Andrew Clarke	Annual review – Personally Identifiable Information replaced with Personal Data (ref DPA 1998 - DPA 2018; Sensitive data replaced with special category data. SALT added to HASH function	07/08/2019
	Andrew Clarke	Annual review	08/06/2020

Document Approval

The contents of this document are classified as Protect to Brunel University London (BUL) information classification. Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.

This document requires the approval from BUL as defined in the ISMS Compliance document.

Owner: Michael Jenkins	Chief Information Security Officer
Signature: MGJ	Date: 26 Jan 2018
Approver: Pekka Kahkipuro	Chief Information Officer
Signature: PK	Date: 26 Jan 2018
Distribution:	

Document Distribution

Name	Title	Version	Date of Issue

Contents

1. About this document

1.1 Purpose of Document

This Policy establishes the area within Brunel University London covering Cryptographic controls.

Please refer to Brunel University London ISMS Document BUL-GLOS-000 - SyOPs Glossary of Terms for the glossary of terms, acronyms and their definitions for the suite of Brunel University London ISMS documentations.

1.2 Responsibilities

Table 1 – responsibilities

Title / Role	Description
Systems Manager	Is responsible for maintaining and managing systems policies on IT systems and infrastructure and ensuring that IS cryptographic controls comply with this policy.
Network Manager	Is responsible for maintaining and managing network policies on network systems and ensuring that network cryptographic controls comply with this policy.
Head of Development and Application Services	Is responsible for implementing cryptographic controls throughout the Software Development Life Cycle
Cyber & Information Security Manager	Is responsible for maintaining Remote Access policy best practice and ensuring compliance with legislative and regulatory requirements.

1.3 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A10 – Cryptography
ISO 27001:2013 Conformance Control	Information Classification Objective A.10.1.1 Policy on the use of cryptographic controls A.10.1.2 Key Management

1.4 Scope

The scope of this policy applies to:

- Brunel University London's personnel, temporary staff, contractors, students and service providers utilising Brunel University London's information system resources;
- Information System resources, including data networks, SAN, LAN servers, PC (stand-alone or network-enabled) and laptops located on Brunel University London and non-Brunel University London locations, where these systems are under the jurisdiction and/or ownership of Brunel University London, and any personal computers and/or servers authorised to access Brunel University London's data networks;

1.4.1 Out of Scope

Exclusions from the scope include Virtual Machine (VM) servers; this does not include VM indirect attached storage which remain in scope.

1.5 References

GPG 3 - Securing Bulk Data Transfers;
GPG 5 - Securing Data At Rest On Laptops;

1.6 Policy Objectives

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that UK regulations and legislation are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the UK.
This policy document sets out principles and expectations about when and how encryption of University digital information should (or should not) be used.

1.7 Policy Overview

Brunel University London information system resources are important business assets that are vulnerable to access by unauthorised individuals or unauthorised remote electronic processes. Sufficient precautions using encryption are required to prevent unwanted access from unauthorised users.

1.8 Policy Maintenance

Supporting standards, guidelines and procedures will be issued on an ongoing basis by Brunel University London. Users will be informed of any subsequent changes or updated versions of such standards, guidelines and procedures by way of e-mail or other relevant communication media. Users shall then have the obligation to obtain the current information systems policies from Brunel University London intranet (IB) or other relevant communication media on an ongoing basis and accept the terms and conditions contained therein.

1.9 Cryptography UK Legislation

Export regulations relating to cryptography technologies are complex. (Any member of the University becoming involved in export of cryptography is advised to seek specialist advice. Cyber & Information Security Services can assist by coordinating access to such advice.)

The Regulation of Investigatory Powers Act (RIPA) October 2000. Section 49 includes a provision for public authorities to demand, where it is judged there are reasonable grounds, decryption keys or decryption of information stored on computer systems in the UK. Anyone who could be assumed to have encrypted and stored data is very strongly advised to ensure that they retain the means to decrypt it.

2.0 Cryptographic Policy

2.1 Policy Summary

- Cryptographic techniques shall be implemented as needed based on a risk assessment in line with the requirements;
- All external communications involving personal data must be encrypted in transit dependent upon the DPIA[1] assessment;
- University or personal information must be protected in line with information security classification guidelines;
- A schedule of all cryptographic controls shall be documented. Access to private keys must be restricted to identified individuals and stored on a network share which only authorised staff, security and IS personnel can access. The server must comply with the requirements for physical protection of assets;
- Brunel University London shall use the United States National Institute of Standards and Technology (NIST) FIPS-140-2 compliant encryption algorithms where appropriate;
- The retention of keys associated with encrypted archives or digital signatures;

2.2 Data encryption for secure network transit

2.2.1 Provided no other restrictions apply, it is permitted for all University staff and students to use computer systems which would normally and by default use encryption, in order to secure data in transit on a communications network.

2.2.2 Whenever possible and appropriate, encryption shall be used to support security of remote access connections to the University's network and computing resources.

2.3 Required use of encryption

2.3.1 Loss, theft, or unauthorised disclosure of certain information could be detrimental to the University, its staff or students. Such information includes that defined as personal data by the Data Protection Act 2018. Where the University is handling digital personal data that cannot be sufficiently secured by physical controls, the data must be encrypted.
Data which must be handled securely, using encryption where pertinent, includes:

- Any personal data classed as “special category” by the Data Protection Act.

[1] Data protection Impact Assessment - is a procedure that describes a data processing and identifies its needs, its adequacy and its risks

- Any data, that is not in the public domain, about a significant number of identifiable individuals.
- Personal data in any quantity where its protection is justified because of the nature of the individuals, source of the information, or extent of the information.

Data as described above must be encrypted:

- Where it is stored on a computing device or any computer storage medium which may be exposed to a significant risk of being lost or stolen. (Computers used to access remotely stored data or to process locally stored data may create cache files. Depending on the technology in use persistent and unencrypted cache files may be created.) Any such device when outside a secure University location is considered to be at significant risk, including home computers.
- Where it is to be transmitted via an external computer network using a mechanism that does not itself incorporate encryption. Depending on the specific technology being used this could refer to: sending data by email either within or outside the University, transferring files offsite, remotely accessing files or Web pages. The risk is that unencrypted data in transit may be intercepted.
- When the data is being sent using a postal service where the data media could be lost, stolen or intercepted and read whilst in transit.

2.3.2 Where data being handled by the University is subject to an agreement with an external organisation specifying use of encryption, the agreed handling procedures, encryption technologies and standards must be used.

2.3.3 Where personal data is to be encrypted and no overriding requirements (from an external body) apply, the recommended minimum University encryption standards (or better) must be applied. For further details refer below to the “Cryptography implementation” section.

2.3.4 Individuals must be authorised by the Head of Department before taking or sending University confidential information out of a secure University location. Optionally the Head of Department may elect to authorise specific individuals to routinely undertake a particular activity involving a specific type of data. A departmental record of such authorisations is to be established and maintained recording the following details:

- The data name or description.
- Who has been authorised to remove the data.
- Purpose for which the data is being removed.
- Date of data removal or an indication where removal is routine, e.g. “during exam marking”.
- Where the data is being taken or sent.
- Any agreed external security requirements that apply to the data.
- Confirmation that the data will be encrypted and handled securely.
- Encryption technology used e.g. name of encryption hardware or software.

If the data being sent off campus is of a personal identifiable nature, the Data Protection Officer must be consulted prior to the release.

2.3.5 University Web transactions that involve the transfer of personal, special category or University Confidential data or funds must use encryption, for

example, Hypertext Transfer Protocol over Secure Socket Layer or Transport Security Layer (HTTPS).

2.4 Management of encryption keys

2.4.1 Departmental procedures must be in place:

- To manage encryption keys in a way that ensures encrypted stored data will neither become unrecoverable nor accessible by an unauthorised person.
- To facilitate authorised officers of the University to obtain prompt access to the encrypted information in the case of an emergency or investigation.
- To ensure that encryption keys are stored and always communicated securely.
- To record who holds encryption keys relating to important information.
- To revoke encryption keys when key holders leave.

2.4.2 Where University information received as email has been encrypted for secure transit, and is information which may be needed again later, it should be securely stored in a form which does not rely on ongoing accessibility of the senders public key.

2.5 Required use of digital signatures

2.5.1 Significant University business information being communicated electronically should be authenticated by use of digital signatures; information received without a digital signature should not be relied upon. Staff involved must assess the level of risk and decide whether to require use of digital signatures or whether to use an alternative means to authenticate the communication.

2.6 Unsupported use of encryption

2.6.1 Staff and students should:

- Not store encrypted data on University systems except where they are able to justify doing so for legitimate purposes.
- Be aware that the University reserves the rights to request sight, at any time, of the unencrypted version of any data stored on its systems and the option to remove any data.

2.7. Cryptography implementation

2.7.1 All encryption products, standards and procedures used to protect University Confidential data must be ones which have received substantial public review and have been proven to work effectively. (see 3.0 algorithm requirements)

2.7.2 Where a department elects to undertake an activity that would incur a cost, in order to remain compliant with security policy, then that cost should normally be found from the departmental budget. For example, where a research project requires measures for secure data handling it is appropriate that costs for any necessary additional security measures are factored into the tender.

3.0 Algorithm Requirements

3.1 Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2, or any superseding documents according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

3.2 Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.

3.3 Signature Algorithms

Algorithm	Key Length (min)	Additional Comment
ECDSA	P-256	Cisco Legal recommends RFC6090 compliance to avoid patent infringement.
RSA	2048	Must use a secure padding scheme. PKCS#7 padding scheme is recommended. Message hashing required.
LDWM	SHA256	Refer to LDWM Hash-based Signatures Draft

3.4 HASH (and SALT) Function Requirements
In general the Brunel University London adheres to the NIST Policy on Hash[2] Functions. It is policy that, where possible, a SALT[3] is added to the hashing process to force their uniqueness, increase their complexity without increasing user requirements

3.5 Key Agreement and Authentication
3.5.1 Key exchanges must use one of the following cryptographic protocols: Diffie- Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).
3.5.2 End points must be authenticated prior to the exchange or derivation of session keys.
3.5.3 Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash.
3.5.4 All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider.
3.5.5 All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

3.6 Key Generation

[2] Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string
[3] SALT is random data that is used as an additional input to a one-way function that "hashes" data, a password or passphrase. Salts are used to safeguard passwords in storage.

3.6.1 Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.

3.6.2 Key generation must be seeded from an industry standard random number generator (RNG).