Cryptographic Controls
Policy & Guidance
Document Control

Document Details

<table>
<thead>
<tr>
<th>Author</th>
<th>Adrian Last</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name</td>
<td>The Crown Estate</td>
</tr>
<tr>
<td>Division Name</td>
<td>Information Services</td>
</tr>
<tr>
<td>Document Name</td>
<td>Cryptographic Controls Policy</td>
</tr>
<tr>
<td>Version Date</td>
<td>14/12/2012</td>
</tr>
<tr>
<td>Effective Date</td>
<td>1 November 2012</td>
</tr>
<tr>
<td>Version</td>
<td>1.7</td>
</tr>
<tr>
<td>ISSUE</td>
<td>THREE</td>
</tr>
<tr>
<td>Review Date</td>
<td>October 2013</td>
</tr>
</tbody>
</table>

Change Record

<table>
<thead>
<tr>
<th>Modified Date</th>
<th>Author</th>
<th>Version</th>
<th>Description of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>15/06/2010</td>
<td>Clare Kelly</td>
<td>1.1</td>
<td>Incorporates changes from TB, CS, ZH, KS and CK</td>
</tr>
<tr>
<td>16/06/2010</td>
<td>Nigel Spencer</td>
<td>1.2</td>
<td>Review and minor format changes</td>
</tr>
<tr>
<td>11/05/2011</td>
<td>Roberta McCaughan</td>
<td>1.3</td>
<td>Edit and Format</td>
</tr>
<tr>
<td>25/05/2011</td>
<td>S Smith</td>
<td>1.4</td>
<td>Reviewed on behalf of Service Desk</td>
</tr>
<tr>
<td>04/08/2011</td>
<td>S Smith</td>
<td>1.5</td>
<td>Final review – see ISMS Action Plan 2011 for info</td>
</tr>
<tr>
<td>11/10/2011</td>
<td>A R Last</td>
<td>1.6</td>
<td>Annual review</td>
</tr>
<tr>
<td>14/12/2012</td>
<td>James Dillon</td>
<td>1.7</td>
<td>Replacement of Safend with BitLocker</td>
</tr>
</tbody>
</table>

Stakeholder Sign–off

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nigel Spencer</td>
<td>Information Services Manager</td>
<td></td>
<td>July 2010</td>
</tr>
<tr>
<td>Clare Kelly</td>
<td>IT Support Manager</td>
<td></td>
<td>July 2010</td>
</tr>
<tr>
<td>Martin Brazier</td>
<td>Knowledge Manager</td>
<td></td>
<td>July 2010</td>
</tr>
<tr>
<td>Nigel Spencer</td>
<td>Head of IS</td>
<td></td>
<td>October 2012</td>
</tr>
</tbody>
</table>

Security Sign-off

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adrian Last</td>
<td>Business Support Manager</td>
<td></td>
<td>July 2010/August 2011</td>
</tr>
<tr>
<td>Adrian Last</td>
<td>ISMS Manager</td>
<td></td>
<td>October 2012</td>
</tr>
</tbody>
</table>
# Table of Contents

1. **Purpose** .................................................. 3  

2. **Scope** ................................................... 3  

3. **Policy** .................................................... 3  
   3.1. Policy Statement ......................................... 3  
   3.2. Policy Objectives ....................................... 4  
   3.3. Policy Overview ....................................... 4  
   3.4. Policy Maintenance ..................................... 4  

4. **Policy Requirements** .................................. 4  
   4.1. General Principles ..................................... 4  
   4.2. Encryption According to Classification .......... 5  
   4.3. Encryption of Data in Transit ....................... 5  
   4.4. Key Management ....................................... 5  
   4.5. Roles and Responsibilities ......................... 5  
   4.6. Encryption for Data Exported Outside the UK 5  
   4.7. Avoiding Adverse Impacts from Encryption .... 5  
   4.8. Reporting Security Incidents ....................... 5  
   4.9. User Awareness ....................................... 5  

5. **Disciplinary Process** ................................ 5  

6. **Deviations from Policy** ............................. 6  

7. **Glossary of Terms** ................................... 6  

Appendix A – List of related documents, procedures and processes 7
1. Purpose

The purpose of this Policy is to protect the confidentiality, integrity and availability of The Crown Estate’s information by applying appropriate levels of cryptographic control.

2. Scope

The scope of this policy applies to:

- Any of The Crown Estate’s premises where electronic information is stored and Crown Estate employees work;
- The Crown Estate’s employees, temporary staff, contractors and service providers utilising The Crown Estate’s information systems; and
- Information system resources, including data networks, LAN servers, personal computers (stand-alone or network-enabled) mobile devices (including Blackberrys, iPads and iPhones), located at Crown Estate offices and non-Crown Estate locations, where these resources are under the jurisdiction and/or ownership of The Crown Estate, and any personal computers, servers and portable computerised media authorised to access The Crown Estate’s data networks. Third parties with access to critical or sensitive data owned by The Crown Estate shall also adhere to this policy.
- Electronic information resources of critical or sensitive data, where:
  - Critical can be defined as information which is of commercial, strategic or significant monetary value to The Crown Estate;
  - Sensitive can be defined as information of which disclosure would either contravene the Data Protection Act or cause measurable damage to The Crown Estate’s reputation or that of its customers or suppliers if it were to fall into the public domain.

3. Policy

3.1. Policy Statement

The Crown Estate’s information system resources are assets important to The Crown Estate’s business and stakeholders and its dependency on these assets demands that appropriate levels of information security be instituted and maintained. It is The Crown Estate’s policy that appropriate encryption control measures are implemented to protect its sensitive or critical information system resources against accidental or malicious destruction, damage, modification or disclosure, and to maintain appropriate levels of confidentiality, integrity and availability of such information system resources.
3.2. Policy Objectives

The objectives of this policy with regard to the protection of information system resources against unauthorised access are to:

- Minimise the threat of accidental, unauthorised or inappropriate access to critical or sensitive electronic information owned by The Crown Estate or temporarily entrusted to it by applying a proportionate level of encryption control;
- Minimise The Crown Estate’s network exposure, which may result in a compromise of network integrity, availability and confidentiality of information system resources; and
- Minimise reputation exposure, which may result in loss, disclosure or corruption of critical or sensitive information and breach of confidentiality.

3.3. Policy Overview

The Crown Estate information system resources are important business assets that are vulnerable to access by unauthorised individuals or unauthorised remote electronic processes. Sufficient precautions are required to prevent unwanted access by applying a level of encryption to critical and sensitive data which is proportionate to the business risk. Users should be made aware of the dangers of unauthorised access, and managers should, where appropriate, introduce encryption controls to prevent such access.

3.4. Policy Maintenance

Supporting standards, guidelines and procedures will be issued on an ongoing basis by The Crown Estate. 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 The Crown Estate Intranet or other relevant communication media on an ongoing basis and accept the terms and conditions contained therein.

4. Policy Requirements

The Crown Estate’s information system resources shall be appropriately protected to prevent unauthorised access by applying a level of encryption to sensitive or critical information which is proportionate to the business risk.

4.1. General Principles

- All critical or sensitive data transferred outside of The Crown Estate should be encrypted.
- All removable media, including memory sticks, should be encrypted.
- Laptop hard drives should be encrypted.
- Portable electronic devices such as Blackberrys, iPads and iPhones should be protected by passwords/PIN numbers.
- All remote access should take place via terminal services.
- Wi-Fi Protected Access encryption is mandatory for all wireless networks carrying The Crown Estate’s data (including domestic networks where remote working is undertaken).
- E-mails (including attachments) should be encrypted whenever sensitive or critical data is contained or attached.
4.2. Encryption According to Classification
All information marked PROTECT, RESTRICTED, CONFIDENTIAL, SECRET or TOP SECRET is to be regarded as sensitive or critical within the context of this Policy.
Information not marked PROTECT, RESTRICTED, CONFIDENTIAL, SECRET or TOP SECRET should still be considered for encryption if it falls within the definitions of sensitive or critical data outlined at clause 3 of this Policy.

4.3. Encryption of Data in Transit
Sensitive or critical data in transit must always be encrypted. Data which is already in the public domain (or would be of no adverse significance if it were to be so) may be sent unencrypted.

4.4. Key Management
The software which force-encrypts removable media employs its own key management system. BitLocker is deployed throughout the business and is managed by the IT Service Desk.
The default media used is memory sticks (flash drives) which can be acquired by contacting the IT Service Desk.

4.5. Roles and Responsibilities
All individuals are responsible for ensuring that sensitive or critical data is encrypted before leaving The Crown Estate’s premises.

4.6. Encryption for Data Exported Outside the UK
Regulatory controls for any country to which data is exported outside the UK should be checked to ensure that cryptographic legislation will not be contravened.

4.7. Avoiding Adverse Impacts from Encryption
Where necessary, encryption keys should be securely managed in a central location such that all information encrypted by The Crown Estate can be decrypted if required.

4.8. Reporting Security Incidents
All security incidents, including actual or potential unauthorised access to The Crown Estate’s information systems, should be reported immediately to the ISMS Manager or Information Services Manager in accordance with the Security Breach and Weakness Policy & Guidance.

4.9. User Awareness
Users shall be made aware of their responsibilities in the prevention of unauthorised access to The Crown Estate’s information resources, including, but not limited to:
The need to encrypt all sensitive or critical data which is to be transported or transmitted;
That suspicious activity is to be reported immediately to the ISMS Manager or appropriate Office Manager;
The need to be aware of this Policy and all its provisions.

5. Disciplinary Process
The Crown Estate reserves the right to audit compliance with the policy from time to time. Any disciplinary action, arising from breach of this policy, shall be taken in accordance with The Crown Estate’s Rules and Disciplinary Code as amended from time to time. Disciplinary action may ultimately lead to dismissal.
6. Deviations from Policy
Unless specifically approved, any deviation from this policy is strictly prohibited. Any deviation to or non-compliance with this policy shall be reported to the ISMS Manager & Information Services Manager.

7. Glossary of Terms
The terms used in this policy document are to be found in the ISMS Glossary of Terms. In particular, cryptographic control is defined as the means of ensuring that The Crown Estate’s electronic information resources are encrypted to a level proportionate to the criticality or sensitivity of each type of information.
Appendix A – List of related documents, procedures and processes

Security Breach and Weakness Policy & Guidance
The Crown Estate’s Rules and Disciplinary Code
ISMS Glossary of Terms