UK SBS
Cryptographic Control Policy

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Owner</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>14-10-2013</td>
<td>Governance and Assurance Manager</td>
<td>Chief of Technology Operations</td>
<td>1st Issue</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Mel Nash)</td>
<td>(Mike Rendall)</td>
<td></td>
</tr>
</tbody>
</table>

Next Review Date | April 2014
Relevant Policies:

Information Assurance Policy
Data Protection Policy
Protective Marking Policy
Managing Security Incidents Policy
Acceptable Use Policy

Contents:

1 Aim and Scope............................................................................................................................... 2
2 Key Principles................................................................................................................................ 3
3 Roles and Responsibilities............................................................................................................... 3
4 Cryptographic Controls.................................................................................................................. 5
5 Contact Information ..................................................................................................................... 3
6 Monitoring and Review ................................................................................................................. 4

Appendix 1: Crypto Control Officer – Key Tasks
1 Aim and Scope

1.1 This policy provides readers with the mandatory requirements for the control of cryptographic items (encryption) used within UKSBS (the company). It applies to all employees and contractors who handle cryptographic items.

1.2 There are to be no exceptions to this policy and breaches may result in disciplinary action being taken.

2 Key Principles

2.1 HMG Information Assurance (IA) Standards No.1 and 2 describe the process to be followed for ICT systems that handle HMG data. The use of cryptographic items must be considered when carrying out risk assessments and accreditation for new and legacy systems. Where HMG (CESG) supplied cryptographic items are used or considered, procedures must be in accordance with HMG IA Standard No. 4 – Management of Cryptographic Systems.

2.2 The level of cryptographic items used must be selected to adequately mitigate appropriate risks. Cryptography will only be used where it adds value. Where the company holds or processes client data, both parties must agree on the level of risk and the cryptographic items to be deployed.

2.3 The appropriate governance of cryptographic items is essential and those involved in the handling of such items must be clear of their responsibilities. The company will ensure that appropriate Personnel Security (vetting) clearance is in place for all users.

2.4 The company will nominate a Cryptographic Control Officer who will be appropriate trained.

2.5 The company will carry out regular inspections to assure compliance with this policy. Sensitive information will be encrypted prior to transmission over unprotected networks or when otherwise deemed necessary.

2.6 Breaches of security involving cryptographic items will be subject to thorough investigation.

3 Roles and Responsibilities

3.1 Senior Information Risk Owner (SIRO). The SIRO is ultimately responsible for information risk across the company. He / she will also request investigations as appropriate and determine the criteria to be met in order to close off any security incidents.
3.2 **Chief of Technology Operations (CoTO).** The CoTO will ensure the correct deployment of cryptographic items and provide management oversight over their use and control.

3.3 **IT Security Officer (ITSO).** The ITSO is responsible for advising on the security of data in electronic form. He / she is responsible for developing and implementing IT Security policy and procedures in accordance with HMG policy standards / guidance and business needs. This must be undertaken in conjunction with the Governance and Assurance Manager, SIRO and those responsible for IT services.

3.4 The ITSO is also responsible for the organisation of IT security, liaison with HMG security and IT authorities on local and national IT security policy issues, providing advice on security reviews and investigations relating to IT issues, as well as being responsible for IT security awareness education and training.

3.5 **Cryptographic Officer (CCO).** The CCO is responsible for developing and implementing cryptographic policy and procedures within the company in accordance with HMG policy and standards (where relevant) and business needs. This must be undertaken in conjunction with the ITSO, Governance and Assurance Manager, SIRO and those responsible for cryptography services (including Service Providers). Where non-HMG items are used, the CCO must develop and implement policy and procedures in line with industry best practice. Key tasks for the CCO are at Appendix 1.

3.6 The CCO will also be responsible for the organisation of cryptographic security, liaison with HMG security authorities, advising security reviews and investigations on cryptographic issues, as well as being responsible for cryptographic awareness, education and training.

3.7 The CCO will work closely with the ITSO, Governance and Assurance Manager, SIRO and Accreditors to ensure overall security is maintained.

3.8 **Governance and Assurance Manager.** The Governance and Assurance Manager is responsible for providing specialist protective security advice and an authoritative insight into the operational application of protective security tools to meet business goals. He / she acts as the Departmental Security Officer (equivalent) and is responsible for day to day security operations.

4 **Cryptographic Controls**

4.1 Cryptographic items must be transported, stored and handled in accordance with their sensitivity.

4.2 All cryptographic items must be subject to proper accounting to cover receipt, issue and destruction (whole life accounting). The accounting must be subject to internal (CCO - monthly) and external (Governance and Assurance Manager - Annually) inspections. Relevant logs must be kept by the CCO and be made available for inspections.

4.3 Any evidence or suspicion of tampering must be reported without delay to the CCO and ITSO.
4.4 Physical security arrangements must be approved by the ITSO. HMG cryptographic items must be stored in SEAP\(^1\) (or comparable standard) approved containers.

5 **Contact Information**

5.1 Further information can be obtained from:

- CCO. Ext 7899
- ITSO. Ext 7899
- Governance and Assurance Manager. Ext 7743

6 **Monitoring and Review**

6.1 The CCO will review this policy annually or as business or legal reasons dictate.

\(^1\) Security Evaluation and Accreditation Panel