## Third Party Security Requirements Policy

<table>
<thead>
<tr>
<th><strong>Overview</strong></th>
<th>This policy sets out the requirements expected of third parties to effectively protect BBC information.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Audience</strong></td>
<td>This policy applies to all third parties and staff, including contractors, temporary staff and suppliers hired by the third party organisation.</td>
</tr>
<tr>
<td><strong>Owner</strong></td>
<td>Head of Information Security</td>
</tr>
<tr>
<td><strong>Contacts</strong></td>
<td>Information Security Policy &amp; Compliance Manager&lt;br&gt;Information.Security @bbc.co.uk</td>
</tr>
<tr>
<td><strong>Updated</strong></td>
<td>28/10/2014</td>
</tr>
<tr>
<td><strong>Other related information</strong></td>
<td></td>
</tr>
</tbody>
</table>
Contents

1 Introduction ........................................................................................................................................... 3
2 Information Security Policy .................................................................................................................. 3
3 Third party organisation ....................................................................................................................... 4
4 Human resources security ................................................................................................................... 4
5 Supplier chain management ................................................................................................................ 4
6 Asset management ............................................................................................................................... 4
7 Physical and environmental security .................................................................................................. 5
8 Facilities and equipment security ....................................................................................................... 5
9 Communications and operations management .................................................................................... 5
10 Access control .................................................................................................................................... 6
11 Information Systems acquisition, development and maintenance .................................................. 6
12 Incident Management ........................................................................................................................ 7
13 Business Continuity Management ..................................................................................................... 7
14 Compliance .......................................................................................................................................... 7
15 Audience Protection ............................................................................................................................ 8
16 Documents ......................................................................................................................................... 8
17 Definitions .......................................................................................................................................... 9
18 Document control ............................................................................................................................... 10
1 Introduction

The BBC relies on the integrity and accuracy of its data in order to deliver its services as stated in its Charter. It is therefore paramount that the integrity, confidentiality and availability of its data are ensured. Any third party which processes or manages BBC Information must adhere to these principles to ensure that the BBC maintains the trust of all relevant stakeholders and remains in compliance with relevant legal and regulatory requirements.

1.1 Purpose

This policy sets out the requirements expected of third parties in order to effectively protect BBC information.

1.2 Audience

This policy applies to all third parties and staff, including contractors, temporary staff and suppliers hired by the third party organisation.

1.3 Scope

The scope of this policy is any third party which will process any BBC Information. This includes, but is not limited to:

- Third parties involved in the design, development or operation of information systems for the BBC e.g. writing and installing bespoke software, third party maintenance or operation of systems, outsourcing of facilities;
- Access to BBC information from remote locations where the computer and network facilities are not under the control of the BBC;
- Users who are not employees of the BBC and require access to BBC information or information systems.

1.4 Information Security Reviews

Third parties must document any security elements and controls that have been implemented to comply with this policy in order to assist with any information security audits carried out by the BBC or nominated parties.

1.5 Exceptions

Where third parties are unable to meet any of the control requirements defined in this policy then approval will be required from the BBC Service Manager and BBC Information Security. Please contact BBC Information Security in the first instance.

2 Information Security Policy

All third parties who are given access to BBC information or information systems must comply with the BBC’s information security policies and associated documentation where appropriate. This policy must also be read in conjunction with the BBC Third Party Security Standards that support this policy and set out baseline requirements where applicable.
A number of BBC Policies are referenced within this document which an external partner is unlikely to have online access to. Critical policies should be sent to the Third Party as supporting documents to this policy, and all others will be available upon request. For this reason hyperlinks to those policies are not included within this document.

3 Third party organisation

3.1 Information security: Third parties must establish a management framework for information security and risk which is signed off at the appropriate level, and ensures the necessary resources to provide required controls.

3.2 Processes and procedures: Documented procedures must be in place to authorise significant changes to agreed BBC Information processing procedures and to ensure relevant information security contracts and controls are maintained.

4 Human resources security

4.1 Prior to employment

4.1.1 Screening: Third party personnel must be subject to appropriate background and vetting checks, depending upon their roles and access levels.

4.2 During employment

4.2.1 Training and awareness: Appropriate information security awareness, training and education must be provided to ensure employees and third parties understand their responsibilities regarding the confidentiality, integrity and availability of BBC information. (Advice and support can be requested from BBC Information Security regarding this requirement.)

4.3 Termination or change of employment

4.3.1 Termination/change: The security of BBC Information must not be compromised as a result of termination of employee or supplier contract, or a change of roles.

5 Supplier chain management

5.1.1 Supplier chain management: Third parties may use suppliers as part of their service to the BBC. Any third party supplier access to BBC Information must be in a controlled and secure manner as required by the BBC Third Party Security Standards.

6 Asset management

6.1.1 Classification: BBC information processed by third parties must as a minimum, be classified in accordance with the BBC’s Information Security Classification & Handling Standard.

6.1.2 Handling: BBC information assets must as a minimum be handled and maintained in accordance with the BBC’s Information Security Classification & Handling Standard.
7 Physical and environmental security

7.1.1 Physical and environmental: BBC Information or systems processing BBC Information must be protected against unauthorised physical access, damage or theft.

8 Facilities and equipment security

8.1.1 Facilities and equipment: Equipment must be secured to prevent loss, damage, theft or compromise of BBC information assets.

9 Communications and operations management

9.1.1 Operating procedure documentation: Operating procedures for information security management and controls related to BBC Information must be documented, maintained and made available to users involved in processing BBC Information.

9.1.2 Separation: Development, test, and production facilities processing BBC Information must be separated to reduce risks of unwanted changes or unauthorised access to live BBC Information. Live BBC Information must not be used in development or test facilities.

Conflicting duties and areas of responsibility must be segregated to reduce opportunities for unintentional or unauthorised modification or misuse of BBC information.

9.1.3 Malware: Controls must be in place to prevent, detect, eradicate and recover from malware threats.

9.1.4 Data back-up: The third party must have appropriate processes in place to recover from the loss or damage of BBC Information or facilities used to process BBC Information. The third party back-up policy must be approved by the BBC Service Manager.

9.1.5 Network security management: BBC Information held in or connected to third party networks including the network infrastructure itself must have appropriate protection.

9.1.6 Platform and application security: Hardware and software used for processing BBC information must provide appropriate protection as outlined in the BBC Third Party Security Standards. Technical security standards for applications used in processing BBC information must be defined, documented and maintained.

9.1.7 System management: Systems security measures must be in place to guard against the accidental, deliberate or unauthorised disclosure, access, manipulation, alteration, destruction, corruption of information through processing errors, damage or loss or misuse of BBC Information.

9.1.8 Mobile computing: A documented policy must be in place to protect against the risk of using mobile computing, teleworking activities and communication facilities where these are used to deliver Services to the BBC.
9.1.9 **Data encryption:** Controls to safeguard the availability, integrity and confidentiality of BBC Information being exchanged, transferred or stored must be established. Any transfer or exchange of BBC Restrict Data must be carried out in a secure manner in compliance with the BBC Data Encryption Policy and Information Security Classification and Handling Standard.

9.1.10 **Monitoring and auditing:** Procedures must be in place to actively monitor for, review, and act on any unauthorised processing of BBC Information.

9.1.11 Auditing of activities and information security events related to the processing of BBC Information must be kept securely, retained as agreed, protected against unauthorised alteration or deletions and backed-up in line with the back-up policy.

10 **Access control**

10.1.1 **Access:** All access to BBC Information and relevant processing facilities must be in a secure and controlled manner as defined in the BBC Third Party Security Standards.

10.1.2 **Passwords:** Password controls must be implemented for all accounts with access to BBC Information or processing facilities. The controls must comply with or exceed the BBC Password Policy.

10.1.3 **Data encryption:** BBC information must be encrypted in line with the BBC Data Encryption Policy.

11 **Information Systems acquisition, development and maintenance**

11.1 **Security requirements for Information Systems**

BBC information security and quality maintenance must be an integral part of information systems:

11.1.1 **Business requirements:** New information systems or enhancements to existing systems must have agreed business requirements which must specify security controls to maintain or protect BBC Information. The business requirements must be agreed by the BBC Service Manager.

11.1.2 **Technical standards:** Technical security standards for applications and systems used in processing BBC Information must be defined, documented and maintained. New systems and applications must comply with these standards.

11.1.3 **Capacity management:** Capacity requirements must take into account the business criticality of the system. Procedures must require information systems to be designed to cope with current and predicted information processing requirements. Regular monitoring and tuning must be applied to ensure required system performance.

11.1.4 **Cryptography:** Procedures for the use of cryptography and key management must be in line with the BBC Data Encryption Policy.

11.2 **Security in development, change and support processes**

The security of applications and systems used to process BBC Information must be maintained:
11.2.1 Change management: Any changes to systems or applications processing BBC Information must be reviewed and tested to ensure there is no adverse impact on business operations or information security. Any major changes must be communicated to the BBC Service Manager.

11.2.2 Secure development: A policy document to outline a secure process for development of software and systems processing BBC Information, whether in-house or outsourced, needs to be defined and maintained.

11.2.3 Source code: Access to program source code must be restricted and strictly controlled.

11.3 Technical vulnerability management

Risks from exploitation of published technical vulnerabilities affecting applications and systems processing BBC Information need to be managed:

11.3.1 Vulnerability and penetration tests: Independent third parties must carry out vulnerability scans and penetration tests on the IT infrastructure used to process BBC Information using a risk-based approach. The results of these tests and any remediation plans must be communicated to the BBC Service Manager.

11.3.2 Patch management: Risk-based procedures for applying security patches and software updates to systems processing BBC Information must be formalised and implemented across the infrastructure.

12 Incident Management

12.1 Policy and Procedure: A documented information security response procedure must be established.

Reporting: Security incidents, issues and control weaknesses related to BBC Information and processing facilities must be identified and communicated in a timely manner to allow for corrective action to be taken.

13 Business Continuity Management

13.1.1 Business Continuity: A Business Continuity Plan in relation to the provision of services to the BBC must be established and as a minimum, meet the requirements set out in the BBC Third Party Security Standards.

14 Compliance

14.1 Data Privacy

14.1.1 Collection, Processing and Disclosure: BBC information processed by third parties must be handled in compliance with Data Protection and Freedom of Information legislation.

14.1.2 Retention: BBC information must be retained in accordance with defined retention periods and only for as long as is necessary for the purpose(s) for which it was collected.

14.2 Legal, Regulatory and Contractual Compliance
14.2.1 **Compliance with requirements:** Legal, regulatory or contractual requirements must be complied with and taken into account in the processing of BBC Information. In particular this includes, but is not limited to compliance with the Data Protection, Freedom of Information, and privacy requirements.

14.2.2 **PCI-DSS:** For provision of financial transactional functionality, the requirements set out in the BBC Third Party Security Standards must be complied with.

14.2.3 **Offshoring:** Any offshoring proposal by the third party supplier or their sub-contractor must be subject to a full information security risk assessment and must be approved by BBC Information Security, Information Policy Compliance (IPC) and reviewed by Technology Legal, before it can proceed.

14.3 **Compliance with BBC Policies and Standards**

14.3.1 **Compliance with security procedures:** BBC Information processing systems including databases processing BBC Information must be checked on an annual basis to ensure they comply with relevant security procedures including this policy.

14.3.2 **Compliance report:** An annual report on the compliance of BBC Information processing systems against the relevant information security standard and this policy must be provided to the BBC Service Manager.

14.4 **Audit**

14.4.1 **Audit Considerations:** In order to ensure compliance and to detect misuse of BBC information systems and or breach of Acceptable Use Policies, Internal Audit and or the BBC Investigation Service may conduct system or process audits when deemed appropriate.

14.4.2 **Audit cooperation:** All users of BBC Information and processing facilities must fully cooperate with any BBC initiated audit activity; this includes audits conducted by third parties on behalf of the BBC.

15 **Audience Protection**

15.1 **Face to face contact:** Where face-to-face contact with BBC audiences and contributors takes place, the requirements of the BBC Third Party Security Standards must be complied with.

16 **Documents**

16.1 **Documents:** Required documents as set out in the BBC Third Party Security Standards must be provided to the BBC when requested to do so.
### Definitions

<table>
<thead>
<tr>
<th><strong>Availability</strong></th>
<th>Ensuring legitimate access to information and associated services is not prevented by unauthorised behaviour (e.g. through Denial Of Service or damage to information).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BBC Information</strong></td>
<td>BBC Information in logical or physical form.</td>
</tr>
<tr>
<td><strong>Business Criticality</strong></td>
<td>Loss of critical processes and systems would result in major impact on the ability of the BBC to continue output or loss of non-priority output</td>
</tr>
<tr>
<td><strong>Confidentiality</strong></td>
<td>Ensuring information is only read by authorised user(s) and not disclosed in an unauthorised manner.</td>
</tr>
</tbody>
</table>
| **Information asset** | 1. A set of data which can be reasonably consolidated into a single group where the contents, media, location, access controls, classification and subsequent impact to the BBC for loss, breach or destruction (temporary or permanent) are the same; or  
2. A single piece of data where it is unique in any of the criteria mentioned in point 1 above and cannot be sensibly grouped with other information. |
| **Information Security** | Maintain the integrity, availability and confidentiality of information. This also includes assuring the authenticity, accountability, non-repudiation, and reliability of interactions with information assets. |
| **Information Systems** | Systems, devices, services (e.g. Internet, email, and telephony), applications and information in logical or physical form |
| **Integrity** | Safeguarding the authenticity and completeness of the information and associated processes through control of who or what can create, update or delete information. |
18 Document control

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Author</th>
<th>Changes/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/04/2013</td>
<td>1.0</td>
<td>AR</td>
<td>Final version (approved by ISCB)</td>
</tr>
<tr>
<td>03/12/2013</td>
<td>1.1</td>
<td>VG</td>
<td>Updated document with policy gaps identified from comparison with the Operational Security Policy. Added Section 15.</td>
</tr>
<tr>
<td>17/12/2013</td>
<td>1.2</td>
<td>VG</td>
<td>Revised policy following document review by Gartner</td>
</tr>
<tr>
<td>21/01/2014</td>
<td>1.3</td>
<td>VG</td>
<td>Updated policy to align with Third Party Security Standards</td>
</tr>
<tr>
<td>09/06/2014</td>
<td>1.4</td>
<td>VG</td>
<td>Added 14.2.3 statement regarding Offshoring</td>
</tr>
<tr>
<td>23/06/2014</td>
<td>1.5</td>
<td>DJ</td>
<td>Minor revisions</td>
</tr>
<tr>
<td>08/08/2014</td>
<td>1.6</td>
<td>VG</td>
<td>Minor rewording and updated formatting for Gateway policy project.</td>
</tr>
<tr>
<td>24/09/2014</td>
<td>1.7</td>
<td>VG</td>
<td>Updated ISGC to BBC Information Security to reflect the change in the team name.</td>
</tr>
<tr>
<td>20/10/2014</td>
<td>1.8</td>
<td>VG</td>
<td>Updated 3.1, 10.1.3 and 14.2.3 following comments from PC</td>
</tr>
</tbody>
</table>