

## DQ Version Information for: Baseline Security Standards for Third Party Suppliers

<b>DQ Status</b>	Live – Overdue for Review		Standard	
<b>DQ Content Authority</b>	Head of IT & Data Assurance (Keith Little)			
<b>Contact(s) for Help</b>	Julia Harris, ISM			
<b>Description</b>	<p><b>Intended Audience:</b> third parties and those dealing with third parties</p> <p><b>Use:</b> This document sets the expected standards for third parties in the management of risks to BBC proprietary information, in</p> <ul style="list-style-type: none"> <li>- information security management</li> <li>- contingency planning</li> <li>- operations security</li> <li>- communications security</li> <li>- personnel security</li> <li>- physical security</li> <li>- auditing and testing</li> <li>- access control and authentication</li> <li>- confidentiality</li> </ul> <p><b>Please Note:</b> as this document is over due for review some content may be out of date, so please contact Julia Harris before using.</p>			
<b>DQ Reference</b>	<b>Version</b>	<b>Date</b>	<b>Last Reviewed</b>	<b>Next Review Due</b>
third_06	01.01	19/09/2000	Sep 2000	Sep 2001 Overdue for Review
<b>Key Words</b>				
<b>DQ Location</b>	Internal: <a href="http://guidelines.gateway.bbc.co.uk/dq/third/baseline.shtml">http://guidelines.gateway.bbc.co.uk/dq/third/baseline.shtml</a> External: <a href="http://www.bbc.co.uk/guidelines/dq/contents/third_parties.shtml">http://www.bbc.co.uk/guidelines/dq/contents/third_parties.shtml</a>			

**BASELINE SECURITY STANDARDS  
FOR  
THIRD PARTY SUPPLIERS TO THE BBC**

*The BBC **insist** on certain base line standards relating to the security of information from its suppliers. This document sets out this expectation and in doing so places on the supplier **a duty of care** to ensure the proper implementation of these standards. If for any reason you are unable to comply with these standards, you must obtain **permission to vary** from these standards from the Head of Information Security and Quality Assurance at [security-manager@bbc.co.uk](mailto:security-manager@bbc.co.uk) . If permission is not obtained from the Head of Information Security and Quality Assurance specifically **the BBC can assume that you are fully compliant**.*

**BBC BASELINE SECURITY STANDARDS FOR THIRD PARTY SUPPLIERS.**

The information to be managed within this service is either BBC proprietary information or belongs to a third party to whom BBC is responsible for its protection. The supplier shall ensure that the service provided has adequate information security protection measures to manage the risks to that information. In the provision of this service, **as a minimum, information security protection** should be included in the following areas:

**1. Information Security Management**

The following requirements are expected to be in place to ensure that there is an appropriate level of information security both within the service to be supplied and within the supplier organisation. Appropriate controls will be required to manage the risks to BBC proprietary

information and that third party information entrusted to the BBC. Furthermore it must be demonstrated that the proposed service fully accords with the BBC Information Security Policy and associated control framework. This will include access controls, authentication, authorisation, audit and review processes.

This is required to protect the service and the BBC from information security incidents throughout the lifecycle of the service.

#### **Supplier Information Security Policy**

The supplier shall have an information security policy that is demonstrable or at the very least a signed commitment to BS7799 and an implementation plan.

#### **The service does not breach the BBC Information Security Policy**

The BBC has an Information Security Policy which is supported at the very highest levels of BBC management. The supplier shall commit in writing that the service to be provided and the suppliers organisation shall not at any time be in breach of the BBC Information Security Policy.

#### **Information Ownership**

The information to be managed, processed or stored within this service is BBC proprietary information *as well as the particular* third party information entrusted to the BBC, it is not intended that it or its title shall pass to the service provider or any other third party. The service provider shall confirm in writing that regardless of the added value he provides to the information the title shall not transfer.

#### **The supplier organisation must have an Information Security Manager**

The supplier's organisation shall nominate an information security manager who will be responsible for the protection of the BBC proprietary information and that third party information entrusted to the BBC as well as ensuring that the information is contained within the bounds of the service provided. This person shall be responsible for liaising with the BBC Information Security Manager and the BBC Chief Investigator.

#### **The supplier has adequate knowledge of information security philosophy**

The supplier shall need to demonstrate that it has a reasonable grasp of the need for security of information and the methods for determining the level of protection required.

**The supplier must have a method of ensuring that information security incidents are properly managed.**

There needs to be an appropriate method in place to ensure that the supplier can properly manage information security incidents as they arise. The service provider will be required to investigate all information security incidents and provide a full report including any action taken to prevent a recurrence. This will be at nil cost to the BBC and within a timescale to be documented within the Service Level Agreement (SLA). This shall include:

- investigation
- escalation
- reporting to the BBC
- feedback into the information security protection measures.

The BBC does not consider that there is any information security incidents that are outside of the requirement for the supplier to report such incidents. The supplier will be required to commit to full openness with the BBC on the investigation and subsequent action taken following information security incidents. BBC would expect as a minimum for procedures to be established covering:

- procedures for disciplinary action
- procedures for legal action

**The supplier must have a policy on the use of illegal software that is acceptable to BBC**

The supplier is required to have a responsible attitude to the Copyright, Designs and Patents Act (1988) as it affects the licensing and use of software. This will include a policy on the management of software and disciplinary procedures to manage any breach of its provisions.

**The supplier shall have appropriate virus checking procedures**

The supplier shall put in place appropriate checking and elimination procedures to ensure that the service is not affected by virus software during development, maintenance and operation. This shall include the certification of all introduced software and new software versions.

**The BBC reserves the right to audit the correct function of all security protection, processes and procedures**

The BBC Information Security Policy Manager, BBC Systems Audit and or their agents shall have the right to inspect the Information Security protection, processes and procedures implemented within the service.

**The supplier shall ensure that the service does not degrade BBC's existing information security countermeasures**

The BBC's existing information security environment shall not be adversely affected by the implementation and operation of the service.

**Ownership of information**

The information within the service is BBC proprietary information and that third party information entrusted to the BBC, it is not intended that it or its title shall pass to the service provider or any third party. The service provider shall confirm in writing that regardless of the added value he provides to the information neither the information nor the title shall transfer.

## 2. Contingency Planning

Contingency planning is the strategic approach to managing security incidents. In an IT context it mitigates the threat to seriously disrupt the availability of an information system or communications service. Because it is strategic, contingency planning should enable the management of every type of incident from a simple software error to a major disaster, where such an incident has the effect of disrupting the availability of information to the business. It seeks to implement **adequate** measures, to manage possible business disruption, which are neither overburdening nor insufficient to meet the business risk.

There must be an agreed, **detailed fallback and recovery plan** within the migration plan to prevent loss or corruption of BBC proprietary information or that third party information entrusted to the BBC.

### **The supplier must provide appropriate contingency provision**

The supplier shall put in place adequate plans and procedures for contingency covering:

- adequate operational contingency
- elimination of single points of failure
- recovery plan
- regular contingency plan review
- staff awareness of contingency
- contingency plan testing
- critical equipment inventory
- safety plans.

### **There shall be a clear definition of responsibilities for action in a contingency situation.**

There shall be a defined set of procedures for action in a contingency situation that shall define the responsibilities. As a minimum the supplier must ensure that:

- supplier responsibilities are fully defined
- BBC responsibilities are fully defined
- third party responsibilities are fully defined.

### **BBC reserves the right to audit the suppliers contingency plan**

The BBC Information Security Policy Manager, BBC Systems Audit and or their agents shall have the right to audit the suppliers contingency plan to ensure they have confidence in its viability. The supplier shall agree to the BBC's right to require changes to the plan if it is found to be inadequate.

### **Proof of the effectiveness of the contingency plan**

The supplier shall provide BBC with evidence to prove the effectiveness of its contingency plan or the BBC shall require the supplier to prove its effectiveness in practice.

### **The supplier shall ensure compatibility between its contingency plan and any BBC contingency plan with which it needs to interface**

The supplier shall ensure that its contingency plan does not compromise any BBC contingency plan nor does it allow gaps to exist in the interface between it and any BBC plans. The supplier must ensure an adequate interface with the BBC business recovery strategy.

### **The supplier must agree to an ESCROW facility for all the provided software**

The supplier must agree to an ESCROW facility for all software supplied under the service contract where this is appropriate. BBC reserves the right to determine where such a facility is appropriate and to whom the responsibility will be passed for the safe keeping of the software.

### **3. Operations Security**

The supplier must convince the BBC that their operation of the service does not compromise BBC information or third party information for which BBC are responsible. This means that there must be adequate standards, processes and procedures in place to ensure that the service is operated according to best practice in operations security. The following requirements shall be met:

#### **The operating system must be configured for secure operation**

The supplier must ensure that all systems that make up the service system are configured in accordance with a recognised standard for operating system security.

#### **The system configuration accords with recognised portability standards**

The systems which make up the service system must all be configured in a like manner and to a recognised portability standard.

#### **All equipment is registered within the asset management system and security marked**

All equipment which constitutes the service system must be security marked to distinguish it from equipment in the control of the BBC. It shall also be controlled and monitored within an asset management system.

#### **The BBC reserves the right to audit the correct function of all operational practices and procedures**

The BBC Information Security Policy Manager, BBC Systems Audit and or their agents shall have the right to inspect the operational processes and procedures implemented for the service. This shall include:

- right to audit logs of operations
- agreement on spot checks of operational procedures
- agreement on right to audit administration procedures
- agreement on right to audit documentation

#### **The supplier must operate the service with a view to good security practice**

The supplier shall at all times operate the service with strict adherence to secure operational standards, processes and procedures. These will include a commitment to:

- least privilege for supervisor access
- audit trail of all supervisor actions
- minimum number of people with privileged access
- ensure adequate audit logs
- user control over access to data
- no software developer access to the live service
- software only loaded by operations staff

#### **The supplier must operate the service with a view to good service management practice**

The supplier shall at all times operate the service with strict adherence to good service management standards, processes and procedures. These will include a commitment to:

- documented escalation procedures for equipment failure
- problem ownership procedures
- procedures for communication with users
- ensure adequate help desk procedures

#### **The supplier shall implement appropriate data management practice**

The supplier shall ensure that appropriate standards, procedures and processes are in place to ensure the proper management of the BBC information. This will include as a minimum:

- nomination of a data manager
- ensure adequate data validation procedures
- ensure adequate database reconciliation
- ensure adequate file conversion controls
- ensure adequate data recovery provisions
- ensure an adequate policy on directory structures

#### **The supplier must ensure that adequate documentation is available to the operations and incident control staff**

The supplier must maintain an adequate supply of appropriate documentation to enable the proper operation of the service. There must also be adequate provision of documentation for the management of incidents.

#### **The supplier shall provide for appropriate procedures for destruction of time expired, faulty or failed media.**

The supplier shall understand the sensitivity associated with all media within the service and put in place appropriate procedures for its secure destruction in case of a fault, failure or life expiry.

## **4. Communications Security**

BBC are defensive of their business network and set a number of conditions on systems that wish to connect to it. These conditions are intended to limit the incidence of:

- unauthorised access to BBC systems
- interference with network components
- performance degradation across the network
- interference with network traffic.

The following conditions apply to all systems wishing to connect to the BBC network:

- network Internet access shall only be through the BBC firewall
- any access to external services shall be controlled at the service point
- any remote access shall be through an adequately secured and authorised route with strong authentication
- any third party gateway between the BBC network and external systems shall be adequately secured
- there shall be controls to prevent unauthorised access from connected systems to the BBC network
- there shall be adequate monitoring and controls to prevent external networks or systems from interfering with the operation of the BBC network.

Systems not meeting these criteria shall not be connected to the BBC network and systems found to be breaching the criteria will be disconnected until re-compliance is guaranteed (a cost may be incurred for reconnection)

## 5. Personnel Security

The supplier shall manage and control its staff on BBC premises and where they have access to BBC information or third party information entrusted to the BBC, in accordance with predetermined criteria for personnel security. This criteria shall be agreed in advance with the BBC. The BBC reserve the right to vet all or any of the implementation and operations team and inspect the service providers staff vetting process for due rigour. All members of the team will be expected to sign a confidentiality agreement in respect of BBC proprietary information and that third party information entrusted to the BBC.

**The supplier shall have appropriate personnel security procedures which are acceptable to BBC.**

These shall as a minimum include:

- procedures for staff vetting
- acceptable standards of behaviour
- disciplinary procedures
- training standards
- succession planning/continuity
- procedures for control of contract staff
- emergency replacement procedures

**The supplier shall have appropriate personnel security procedures for handling incidents relating to operational personnel.**

The supplier shall have procedures in place to manage the following personnel issues:

- dismissal
- resignation
- redundancy
- termination of contract
- transfer
- death in service
- exit interviews
- staff removal from building
- removal of user IDs
- removal of identity badges
- keys returned
- PINs disabled

## 6. Physical Security

The service provider will be required to implement appropriate physical and environmental control to protect the service. The BBC reserves the right to conduct periodic audit checks on the physical security environment provision the first being before any go live date.

The following minimum standards are to be implemented in any accommodation of the service equipment:

- all equipment to be housed in unoccupied areas
- equipment area to be physically secured with controlled access
- hand held fire extinguishers easily accessible
- automatic fire suppression equipment in place
- appropriate fire detection equipment installed
- smoke detection equipment installed
- water detection equipment as appropriate
- appropriate power supply cleanliness and contingency
- appropriate environmental controls
- appropriate regular cleaning regime
- complete absence of paper (including documentation) and other combustibles
- absence of non-utilised equipment
- cables properly managed
- cables properly labelled
- telephone with emergency numbers prominently displayed
- contingency plan initiation sequence prominently displayed
- location of backup media prominently displayed close to associated equipment
- incident logs are provided, clearly marked and accessible

### **The supplier must ensure that responsibilities for maintenance of the operating environment are properly managed**

The supplier must put in place appropriate procedures to ensure that the responsibilities for the maintenance of a secure operating environment are properly allocated and discharged.

### **The supplier must ensure adequate procedures for the protection of the service equipment**

The supplier must ensure that adequate procedures are in place for the physical protection of the service equipment. This must as a minimum cover:

- intruder(s)
- fire
- water
- environmental (storm etc.)
- physical damage (accident)
- physical damage (deliberate)

## 7. Auditing

The auditing of events on IT systems is intended to identify security related incidents to enable the tracking of causes and the effects. This will allow for damage limitation in the short term and prevention in the future. Audit events are not only error or exception events but are also normal occurrences that are used to track the lead up to security incidents.

### **The supplier shall ensure adequate auditing of occurrences on the service**

The supplier shall ensure that there are adequate provisions for the logging of events on the service to record as a minimum:

- legitimate access
- authentication exceptions
- authority exceptions
- privilege changes
- data object owner changes
- export of information
- out of hours access

### **The supplier must ensure adequate monitoring of audit trails**

The supplier must ensure that audit trails are regularly and effectively inspected for information security incidents. The BBC Information Security Policy Manager, BBC Systems Audit and or their agents shall have the right to inspect the processes and procedures implemented for the monitoring of the service audit trails.

### **The supplier must ensure the investigation of all information security incidents identified through audit trail monitoring**

The supplier must have processes and procedures in place to manage the investigation and subsequent action to be taken in response to the identification of information security incidents in audit trails. This shall be controlled within the overall policies established for the management and reporting of information security incidents as described above.

## 8. Testing

### **The supplier shall provide BBC with evidence of an adequate testing regime**

All software supplied to BBC for use on the service system shall be adequately tested. These tests shall be managed within a structured testing regime which shall include as a minimum:

- functional testing
- integration testing
- security testing
- performance testing
- acceptance tests
- independent test authority
- independent testing
- regression testing of system software version compatibility

### **There must be adequate certification and acceptance provision**

The supplier must have procedures in place to ensure the proper certification and acceptance of products after testing. This will include as a minimum;

- customer acceptance
- design authority acceptance
- test certification
- customer handover procedures

### **The supplier must have adequate procedures in place for the management of test data**

The supplier must demonstrate that its testing regime is able to adequately manage test data.

BBC does not encourage the use of live BBC information for testing purposes. If this is essential to the successful implementation of the service the supplier must demonstrate that there are adequate procedures in place to manage the use the of live information

Equally BBC do not encourage the use of sensitive information in testing. If this is essential to the successful implementation of the service, the supplier must demonstrate that there are adequate procedures in place to manage the use the of sensitive information

## **9. Access Control and Authentication**

Access control and authentication are important for the service system due to the confidentiality of the information processed and the wide range of users present. There is no predicated method of access control and authentication within the BBC or the service and any method will be considered provided that evidence of its integrity can be provided.

The de facto industry standards for access control and authentication (UIDs and Passwords) are not considered to be adequately secure without preconditions so the following conditions are to be set on their use:

- no indication of ID and password requirements on screen
- password length of at least 8 characters including:
  - alpha numeric and special characters
  - case sensitive syntax
  - computer held list of denied passwords
  - checks to identify weak passwords option
  - 3 login attempts only before lockout
  - reuse of passwords prohibited for at least 10 changes
  - date and time of last access display
  - system generated password option
  - system forced password expiry
  - time scheduling of sessions option
- no echoing or storage of passwords in clear text
- double passwords for sensitive information
- screen blanking and reauthentication on time-out
- reauthentication after line or system failure
- user IDs and passwords disabled after a period of disuse

## 10. Confidentiality

The supplier will need to demonstrate that the information security regime proposed to protect the service information is appropriate to the ambient risks. Furthermore it must be demonstrated that the proposed service fully accords with the BBC Information Security Policy and associated control framework.

### **The supplier must implement protection measures to ensure the confidentiality of the service information**

The supplier is expected to implement protection measures to ensure the confidentiality of BBC proprietary information and that third party information entrusted to the BBC and stored within the service. This may include:

- adequate file/record access controls
- encryption of sensitive files
- line encryption
- secure key management
- policy on directory structures
- least privilege
- need to know authorities
- use of Access Control Lists (ACL)

### **Data Protection Act (1998)**

It is expected that the information processed within this service will require to be registered and protected within the provisions of the Data Protection Act (1998).

The service provider will need to demonstrate that:

- he has the appropriate registration(s) to operate within the scope of UK law
- the information security regime proposed to protect this information is appropriate to the legal requirements
- his staff are advised of their responsibilities under UK and European law.

The supplier is expected to understand and responsibly accept his obligations under these legal requirements this will include:

- subject access procedures
- access without the data users authority
- procedures for handling DPA exceptions
- especially sensitive data handling

