

Making Security Second Nature

Holding and hosting requirements gathering form

Intended Audience	Anyone intending to host BBC information away from the BBC infrastructure Use: Form for completion. The form covers requests to hold and host both personal and non-personal data held on an external ISP, or other data processor.
Document Authority	BBC Information Security
Contacts for document:	Pete Juzl and Andrew Sands
Version information:	This version published July 2011

Background

BBC Information Security are required to assess the adequacy of security controls for all systems/projects/services that host BBC data, prior to those systems going live. Increasingly those systems are hosted by third party organisations, off our network.

Before you start – please be aware that when looking at a new 3rd party hosted system or service, you must have first considered whether existing BBC in-house capabilities are able to deliver what you need.

About this form

You've been asked to fill in this form because you are involved in planning a new system which will process/host BBC data outside of the BBC network, or are intending to make changes to one that already exists. Where technical expertise is required, we expect relevant technicians to be consulted to provide accurate answers.

The answers should be provided by a combination of staff from the third parties involved, and the internal BBC staff responsible for the project, depending on where the necessary understanding resides.

Where the system is not affected by questions in this form, you are at liberty to mark these N/A, but please detail why you believe these are not applicable.

There are no right or wrong answers to this document. It is used to assess your security capabilities in the context of the system/service being delivered, and in particular the sensitivity of the data being hosted. Small organisations are not precluded, and a single person may be responsible for many roles that appear to be defined within these questions.

Once you have completed the form, please submit it to BBC Information Security (is@bbc.co.uk), who will review the form and ask further questions as required to complete their review. Based on this review, BBC Information Security may require additional controls/mitigations to be implemented as a condition for signoff.

Please ensure you are using the current version of the document which is located:-

on Gateway :- [IS Approval Forms page](#) [explore.gateway.bbc.co.uk]

on bbc.co.uk :- [DQ Third Party Policies page](#) [bbc.co.uk]

1. Summary information about system/project under review

1.1	Please enter your name, contact details and your role with this project or system	
1.2	Please detail the name of the BBC contact and their details.	
1.3	If the system, solution, project or development has a name, please indicate it here: We sometimes encounter systems that have previously been known as something else, if this is the case, please let us know any previous names:	
1.4	If your submission is part of a larger system or project, please give the name of the "parent" system or project. If you have already submitted one of these forms for the parent system, please indicate this here, and only answer the rest of the questionnaire if there is a difference between this child system and its parent. If the submission is replacing an older system – please explain here how the data / crypto keys on this system will be securely destroyed/migrated.	
1.5	Please give an indication of how urgent the Information Security approval is – and indicate any critical decision dates:	
1.6	If the system were to become non-operational as a result of a security event that affected it (or dependent systems), would this impact broadcast output or the ability of the BBC to perform its normal business functions? Please explain how: Similarly, if information were to become stolen from the system, or modified/deleted as a result of a security event, would this impact broadcast output or the ability of the BBC to perform its normal business functions? Please explain how:	

2. High-level details

2.1	Please give a very brief description of what the system is for and how it will work	
2.2	Please describe the information/data that is stored/processed by the system. <i>(If you are collecting or processing any personal data (including name, email, address, mobile, DOB, age, bank details, staff number, salary, NI number, next of kin, images, nationality, race, gender, criminal record, religion, sex life, political opinion/affiliations, IP addresses) you must fill out the data map in Appendix A)</i>	
2.3	Please can you supply us with a reasonably detailed diagram of the information flows within the system and between it and other systems?	
2.4	Please can you supply us with a high-level system diagram showing what equipment will be used, where it is located and how it is inter-connected? <i>(This can be the same diagram as above if it covers both clearly.)</i>	
2.5	Does the system accept data from another system and if so, what? Does the system send data to another system and if so, what?	
2.6	What are the principle methods of transporting information? <i>Examples include (but are not limited to): HTTP "get"; SFTP over SSH; HTTPS; email etc.</i>	
2.7	Is your requirement likely to need a name registered on the Internet? If yes – you must contact domain.manager@bbc.co.uk [Domain Manager in the GAL] to manage this process.	
2.8	(BBC Internal Question) Has any funding been allocated to secure the solution	

Please ensure you are using the current version of the document which is located:-

on Gateway :- [IS Approval Forms page](#) [explore.gateway.bbc.co.uk]

on bbc.co.uk :- [DQ Third Party Policies page](#) [bbc.co.uk]

2.9	(BBC Internal Question) Who in the BBC will be responsible for controlling access to the data after go-live? (e.g. who is the data owner)	
2.10	Most systems need to be operated, supported, maintained and repaired. What plans are in place to perform these functions? Which group(s) or suppliers will be responsible?	
2.11	Are you ISO 27001 compliant? If not, are you aiming to become ISO 27001 compliant, and when by?	
2.12	What is the contract period for each 3 rd party?	
2.13	What audit rights will the BBC have in the contract with the supplier?	
2.14	Will the data be shared with any other third parties? If so have you audited the third parties to determine whether they have implemented appropriate security measures?	

3. Support Responsibilities Matrix

	INFRASTRUCTURE SUPPORT LAYER	NAME OF RESPONSIBLE ORGANISATION/INDIVIDUAL (or N/A)
3.1	Physical Hardware/Data Centre (Computers, Network infrastructure, Power and Cooling)	
3.2	Virtualisation Layer Support (where applicable)	
3.3	Operating System Support	
3.4	Database Support (DBAs)	
3.5	Application / Web Application Support (Code)	
3.6	Application / Web Application Support (User Admin)	

4. Information Security Policy

Comply
Y/N?

4.1	Please provide a copy of your high level information security policy (For very small organisations, a brief statement outlining your approach to information security may suffice.)	
4.2	If the body holding the data is a subcontractor to the body which has the contract with the BBC, can we please also have the Information Security Policy of the contracted party?	
4.3	Who are the owner(s) of your security policy? (names and positions please) (Very small organisations – who is responsible for information security in your business)	

Please ensure you are using the current version of the document which is located:-

on Gateway :- [IS Approval Forms page](#) [explore.gateway.bbc.co.uk]

on bbc.co.uk :- [DQ Third Party Policies page](#) [bbc.co.uk]

4.4	Is there a management body to ensure adequate information security, and if so who chairs it (include job title)?		
4.5	How is the Information Security Policy communicated to all staff?		
4.6	Is the Information Security Policy regularly reviewed? When was the last time it was amended?		

5. Physical, Hardware and Network			Comply Y/N?
5.1	Where are the servers which will hold the BBC data? <ul style="list-style-type: none"> all in the UK some in the UK (where are the rest?) none in the UK (where are they?) 		
5.2	How do you control physical access to your information processing facilities? Are there physical entry controls to all areas holding BBC data, consider <ul style="list-style-type: none"> server rooms paper records backup facilities tape/disk storage 		
5.3	Will any hardware be stored outside of locked server rooms?		
5.4	Will this system require the installation of any hardware devices on BBC premises?		
5.5	Please describe how BBC data is kept logically and/or physically separated from other users' data?		
5.6	What firewalls or network control measures (e.g. IDS) are in place to protect the system/data? Describe how you configure, maintain the above, and monitor alerts generated.		

6. Software (including operating systems and databases)			Comply Y/N?
6.1	Please indicate what operating systems (including virtualisation environments) will be running on the systems holding and processing BBC data.		
6.2	What process and procedures will be applied to remove unnecessary services from running automatically on each of the operating systems (a process known as "hardening")?		

Please ensure you are using the current version of the document which is located:-

on Gateway :- [IS Approval Forms page](http://explore.gateway.bbc.co.uk) [explore.gateway.bbc.co.uk]

on bbc.co.uk :- [DQ Third Party Policies page](http://bbc.co.uk) [bbc.co.uk]

6.3	Please outline your approach to security patching of operating systems and applications that form part of the system. Please confirm that critical and important security patches are up to date.		
6.4	Please give details of any databases that form part of the system.		
6.5	Please give details of any encryption applied to data at rest on the system (including within database tables). How will the keys be stored, transferred or revoked?		
6.6	Please confirm that all pre-installed system account passwords have been changed from their defaults.		
6.7	Please outline any anti-malware (antivirus, etc) tools used to protect the system.		

7. Access Control			Comply Y/N?
7.1	Please describe the logical access routes available to access this system, describing how users and system administrators uniquely identify themselves. <i>e.g. User login with password over web, Admin login over private network/at console using private key</i>		
7.2	User Accounts Please state what system enforced password settings are active for: <ul style="list-style-type: none"> • Password Minimum Length/Complexity • Password Change Interval • Lockout (after incorrect password entries) 		
7.3	Administrator Accounts Please state what additional measures are in place to secure administrator accounts. (e.g stronger passwords or crypto keys required to access systems)		
7.4	How many people will be administrators and have the ability to make changes to the system's functionality (e.g. add users, delete/modify/view information they themselves did not create)? Of this number, how many will be involved in administering the Operating Systems/Servers? Of this number, how many will be involved in administering the application/service?		
7.5	Are there any generic logons with access to BBC data?		

Please ensure you are using the current version of the document which is located:-

on Gateway :- [IS Approval Forms page](http://explore.gateway.bbc.co.uk) [explore.gateway.bbc.co.uk]

on bbc.co.uk :- [DQ Third Party Policies page](http://bbc.co.uk) [bbc.co.uk]

7.6	How have all those with access to BBC data, whether staff, contractor or temporary, been adequately vetted on recruitment. Please describe any additional vetting carried out on administrators.		
7.7	Joiners / Movers / Leavers Please describe the processes you have in place to manage joiners, movers and leavers. E.g. Revocation of rights, deletion of obsolete accounts, approval of permissions etc.		
7.8	Who is responsible for ensuring that logical access rights are up to date and maintained to: <ul style="list-style-type: none"> • The operating system; • The database; • The application 		
7.9	How are security incidents managed and reported to the BBC? Are all those with access to BBC data made aware of when to and how to report incidents?		
7.10	What is the organisation's approach to those who commit security breaches?		
7.11	If relevant, how do other applications or systems that need to gain access to the data uniquely identify themselves?		
7.12	How does the system hand out the necessary privileges needed for an individual to do their job? How does it prevent people or systems accessing material or information if they don't have the right?		
7.13	If relevant, how does the system hand out the necessary privileges for another application or system to gain the correct access to information? How does it prevent access to the wrong material?		
7.14	Can you detect unauthorised access to BBC data? If you do, what will you do with the information obtained? Can you tell whether the data was viewed, altered or deleted?		
7.15	What logs are kept of successful/unsuccessful usage attempts?		

8. Disaster recovery, backups and data erasure		Comply Y/N?
8.1	(BBC Internal Question) If the system is affected by an external event, how long can it be unavailable before it causes significant disruption to BBC operations.	
8.2	What method will be put in place to secure archive historic material and data?	

Please ensure you are using the current version of the document which is located:-

on Gateway :- [IS Approval Forms page](#) [explore.gateway.bbc.co.uk]

on bbc.co.uk :- [DQ Third Party Policies page](#) [bbc.co.uk]

8.3	What methods will be put in place to securely back-up the system (and securely store the back-ups)?		
8.4	How will the system be restored (either from backup or a rebuild from scratch) to a known working state? And how has the restore process been tested?		
8.5	If the contract with the BBC requires a high availability level (say 95% availability or above), how do you secure against: <ul style="list-style-type: none"> • Power outage • Single points of failure • Unavailability of critical staff • Unsatisfactory maintenance of equipment • Failure of equipment/software 		
8.6	Please describe how BBC data will be securely destroyed when no longer needed		

9. Web Application Security		Comply Y/N?
If the system incorporates any web application functionality – please complete this section. (If not – please put N/A)		
Understanding Data Flows / Interactivity		
9.1	Please outline what the web application actually does (functionality etc)	
9.2	Describe core user journeys.	
9.3	What data does the web application store? Does this include: personal data, childrens data, confidential BBC data? IF yes – you MUST complete Appendix A in full, taking care to fully describe the data in detail.	
9.4	Will the web application collect and/or host any User Generated Content (UGC)? If so – describe the UGC in detail and explain what moderation approach is applied?	
Technical		
9.5	Where will the web application be hosted? (Siemens, Forge, Other BBC controlled, Third Party hosting)	
9.6	BBC controlled hosting only. If the web application is to be hosted on the Platform (Forge) – or contains elements that links to Platform delivered web content – you must complete a CIS ticket. https://confluence.dev.bbc.co.uk/display/CIS/Compliance+and+Information+Security Please provide a link to your ticket.	

Please ensure you are using the current version of the document which is located:-

on Gateway :- [IS Approval Forms page](#) [explore.gateway.bbc.co.uk]

on bbc.co.uk :- [DQ Third Party Policies page](#) [bbc.co.uk]

9. Web Application Security		Comply Y/N?
If the system incorporates any web application functionality – please complete this section. (If not – please put N/A)		
9.7	<p>Are users of the application required to login?</p> <p>Is this login over a secure link – e.g. HTTPS?</p>	
9.8	<p>Please describe any other data transfers / connections between users' browsers and the web application?</p> <p>e.g. Cookies, Form submissions etc</p> <p>Please explain how these data transfers are secured in transit (e.g. HTTPS - SSL/TLS etc)</p>	
9.9	<p>Please describe the web application solution stack?</p> <p>E.g. LAMP – Linux > Apache > MySQL > PHP</p> <p>WINS – Windows > IIS > .NET > SQL Server</p>	
9.10	<p>Please outline your approach to identifying applicable security patches and applying these to the web application solution stack.</p> <p>Please confirm that the solution stack is fully up to date in terms of critical and important security patches.</p>	
9.11	<p>The following list is the OWASP top ten list of web application security issues (as at 2010)</p> <p>A1: Injection A2: Cross-Site Scripting (XSS) A3: Broken Authentication and Session Management A4: Insecure Direct Object References A5: Cross-Site Request Forgery (CSRF) A6: Security Misconfiguration A7: Insecure Cryptographic Storage A8: Failure to Restrict URL Access A9: Insufficient Transport Layer Protection A10: Unvalidated Redirects and Forwards</p> <p>Please confirm what processes you have in place to minimise the risk of these issues being present in your web application.</p> <p>E.g.</p> <p>How have you ensured your developers are capable of writing secure code / identifying vulnerabilities?</p> <p>What approach do you take to code review (e.g. by peers / software tools / independent audit)?</p>	
9.12	<p>Please indicate whether any vulnerability scanning or penetration testing has been carried out on the application?</p> <p>If so – please indicate any critical or significant findings from such reviews and how you have addressed them.</p>	
9.13	<p>Please outline firewalling strategy for web application (attach a diagram if you have one)</p> <p>Is a web application firewall in place? (i.e. a firewall which prevents inappropriate input from reaching the application)</p>	

Please ensure you are using the current version of the document which is located:-

on Gateway :- [IS Approval Forms page](#) [explore.gateway.bbc.co.uk]

on bbc.co.uk :- [DQ Third Party Policies page](#) [bbc.co.uk]

9. Web Application Security		Comply Y/N?
If the system incorporates any web application functionality – please complete this section. (If not – please put N/A)		
Hosting/Capacity		
9.14	How have you ensured the data links to the web server are adequate for traffic volumes anticipated?	
	Have you tested under anticipated load?	

Appendix A - Personal Data Processing Activities - Data Map

This data map must be completed if you are collecting or processing any personal data (unless you have already completed a standalone data map on request from Information Policy & Compliance (IP&C)). Please provide as much information as possible.

The map is on the following page.

Any personal data being held on behalf of the BBC is subject to the Data Protection Act 1998. The BBC's registration number is Z517352X and it can be viewed on the Information Commission's web site at <http://www.informationcommissioner.gov.uk/>.

There are three options under the Data Protection Act:

1. The BBC is the data controller, and therefore is responsible for the security of the data. The third party is a processor.
2. The third party is the controller, and the BBC restricts use of the data under the contract. If this is the case, this **must** be stated on the site collecting the data.
3. The BBC and the third party are joint data controllers. This **must** be stated on the site, and the BBC and the third party have to set out their relative responsibilities and the use to which the data can be put in the contract.

Please ensure you are using the current version of the document which is located:-

on Gateway :- [IS Approval Forms page](#) [explore.gateway.bbc.co.uk]

on bbc.co.uk :- [DQ Third Party Policies page](#) [bbc.co.uk]

Companyname

BBC

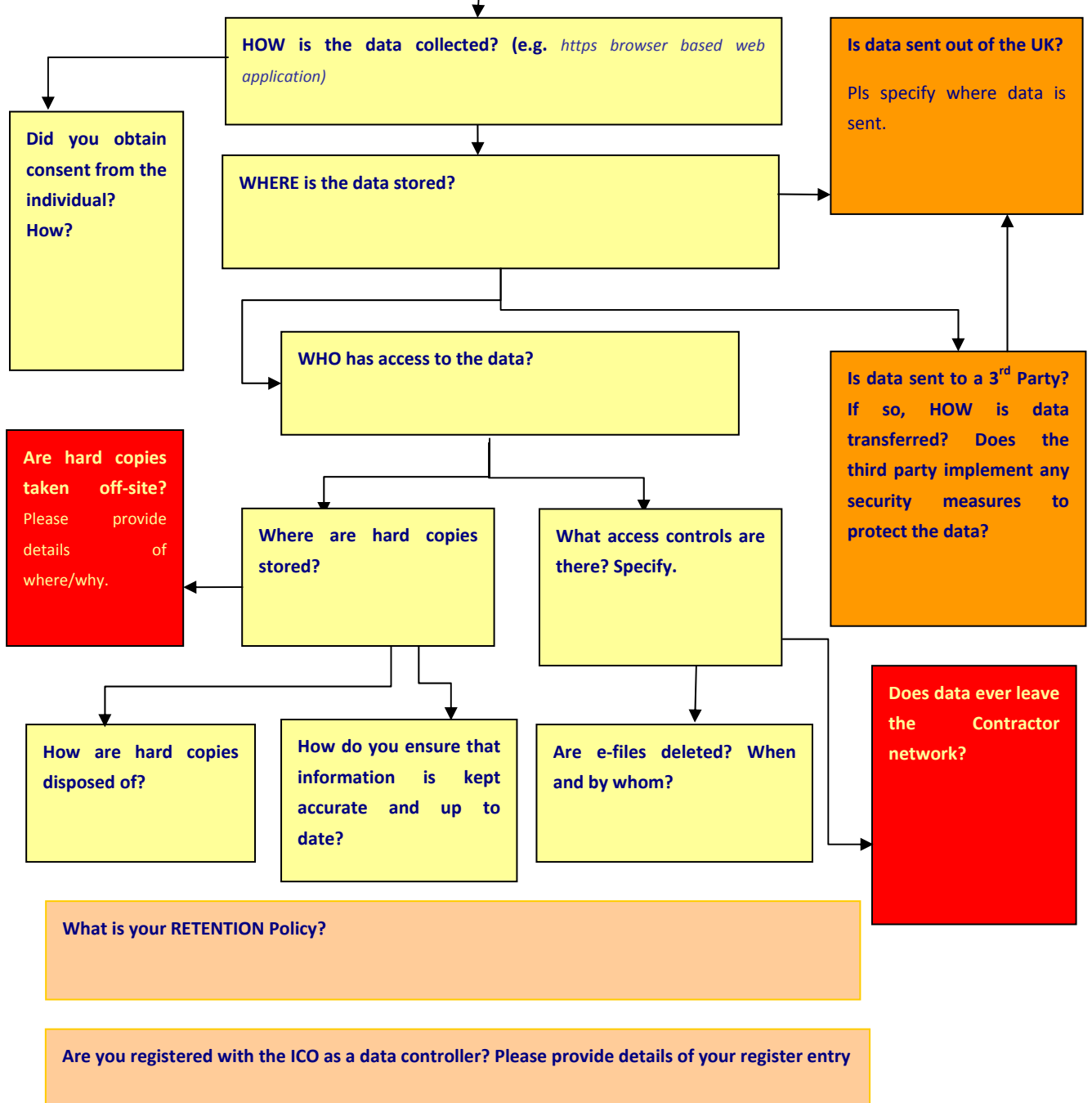
System name

Contract between BBC and contractor



Contact details: Name / Email / Phone

WHAT data is collected and WHY?
Please identify what exactly is collected and why you need it.



Please ensure you are using the current version of the document which is located:-

on Gateway :- [IS Approval Forms page](http://explore.gateway.bbc.co.uk) [explore.gateway.bbc.co.uk]

on bbc.co.uk :- [DQ Third Party Policies page](http://bbc.co.uk) [bbc.co.uk]