BBC Third Party Information Security Requirements – BBC Data

Last reviewed: 14/03/2023

Policy owner: Chief Information Security Officer

Department: BBC Information Security

Summary

This document sets out the minimum security requirements expected of third party organisations who have access to, process, or store BBC information during the provision of contracted or commercial services to the BBC.

This document aims to protect BBC information by providing a flexible yet consistent approach to managing information security risk in third party suppliers and partners, and assist BBC suppliers and partners to better understand and work co-operatively with the BBC on proportionate security controls.

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

Contents

BBC Third Party Information Security Requirements

1. Introduction

The BBC relies on the integrity and accuracy of its data in order to deliver its services as stated in its Charter, and to enable subsidiaries to fulfil their commercial objectives. It's therefore essential that the confidentiality, integrity and availability of BBC data is ensured. Any third party that has access to, processes, or stores BBC information must adhere to this document to ensure that the BBC maintains the trust of all its stakeholders and remains compliant with relevant legal and regulatory requirements.

1.1 Scope

This document sets out the minimum security requirements expected of third parties who have access to, process, or store BBC information during the provision of contracted or commercial services to the BBC. It is not intended to be an all-inclusive list of security controls, and there may be specific security requirements that are generated as part of an individual solution. Where this is the case, the Third Party will be notified and BBC Information Security will work with the Third Party to achieve an appropriate outcome.

The scope of this document includes any third party organisation (including subcontractors appointed by the third party) that will have access to, process, or store BBC information, with the exclusion of BBC Studios content which is subject to the BBC Studios Content Security Assessment Policy and procedure.

2. Information security governance, policy and standards

2.1 The Third Party must maintain an Information Security Management System (ISMS) or set of information security policies that define responsibilities, are approved by senior management, and set out the Third Parties approach to information security in line with industry recognised standards or frameworks (e.g. ISO27001, NIST).

2.2 The Third Party must designate named individuals or teams who will have responsibility and accountability for information security policy, implementation and processes/procedures. Those nominated should act as the primary point(s) of contact for the BBC where information security is concerned.

2.3 The Third Party must ensure that its information security policies are published, kept up to date and effectively communicated to all staff responsible for accessing, processing or storing BBC information.

2.4 The Third Party must have documented procedures in place to authorise any significant changes that might impact the security of BBC information, and to ensure that relevant information security contacts are maintained.

2.5 The Third Party must maintain safeguards against the accidental, deliberate or unauthorised disclosure, access, manipulation, alteration, destruction, corruption, damage, loss or misuse of BBC information in the possession of the Third Party or any sub-contractors of the Third Party.

2.6 The Third Party must maintain a register of any identified security risks related to the provision of its services to the BBC and to BBC information. Risk assessments carried out by the Third Party under its contractual obligations should involve a senior individual with overall responsibility for information security. The risk register should be produced in consultation with the BBC service manager and BBC Information Security, and maintained to show the nature, extent of, and progress made, in mitigating the identified risks to ensure that BBC requirements are met.

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

2.8 The Third Party must have a documented policy in place to protect against the risks of using mobile computing and remote working activities where these are being used to deliver Services to the BBC.

3. Human resources security

3.1 The Third Party must ensure that information security roles and responsibilities of all employees and contracted individuals are clearly defined, documented and understood. This includes information security responsibilities that remain valid after termination or change of employment.

3.2 The Third Party must have a disciplinary process in place that clearly defines what breaches of security represent misconduct and what consequences shall be incurred as a result of a security breach.

3.3 Third Party personnel must be subject to background and vetting checks in line with any relevant laws, regulations and ethics. The background checks must be proportionate to business requirements, the classification of information to be processed and the perceived risks.

3.4 Information security awareness, training and education must be provided to all third party employees (including freelancers/contractors) as relevant to their role. As a minimum, such training should include information protection and security, password and user account security, legal and regulatory (e.g. GDPR/Data Protection) requirements and the established policies, standards and procedures of the organisation, as well as testing of understanding.

4. Asset management

4.1 The Third Party must record all hardware assets (e.g. desktops, laptops, tablets and mobile phones) in an inventory where the assets are used to process or store BBC information. The inventory must be maintained and kept up to date. All such assets must have a designated owner.

4.2 The Third Party must document and implement an Acceptable Use Policy (AUP) for information and assets associated with the processing of information. This must be kept up to date and communicated to users accessing or processing BBC information.

4.3 The Third Party must ensure that information is classified consistently in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification. BBC classifications can be found in Appendix A of this document for reference; however, third parties are not required to adopt the BBC's Classification scheme. If requested, third parties must make their classification policy available to BBC Information Security to confirm that it meets best practice.

4.4 The Third Party must develop and implement an appropriate set of procedures for the labelling of information and the handling of assets in line with the information classification scheme adopted by the Third Party (and its subcontractors).

4.5 The Third Party must ensure that any removable media (including but not limited to USB drives, CD's, DVD's or other magnetic media) used to record, store or process BBC information, is authorised to be used under the Third Party's information governance policies and procedures. It must be securely handled, transported, encrypted and disposed of in accordance with the classification scheme adopted by the organisation.

4.6 BBC Information stored in physical or electronic form must be destroyed or deleted securely (see section 7.5), appropriate to its associated risk, ensuring that it is not recoverable.

5. Access control

5.1 The Third Party must have a documented Access Control Policy for providing access to Third Party systems, BBC systems and BBC information. The policy must be regularly reviewed and kept up to date to ensure that access is limited to only those personnel that need access to such information or systems to perform their duties.

5.2 The Third Party must ensure that all platform and application user accounts are unique i.e. one account per user, with no accounts shared between more than one user. All such accounts must be authorised, regularly reviewed with access revoked when no longer required, and:

- only granted minimum privileges needed;
- access to audit trails is restricted and logged;

- default accounts are deleted or disabled if not required;
- individuals must not be able to approve their own access;
- privileged platform accounts e.g. root are only used under change control procedures and not for day-to-day use;
- all privileged access should be logged in a way that is traceable to ensure operational accountability; and
- where privileged account access is used, approval and use must be documented and regularly reviewed.

5.3 The Third Party must ensure that the identity of a user is established and verified before providing new, replacement or temporary passwords. .

5.4 The Third Party must have a system-enforced password and user account policy that includes as a minimum:

- Passwords for user accounts must be at least 8 characters in length and contain both letters and numbers.
- Wherever possible new user accounts must be configured with a one-time use password which the user is forced to change after their first login.
- Passwords for privileged user accounts (administrative accounts) must be at least 15 characters in length and contain a mixture of upper case letters, lower case letters, numbers and special characters (i.e. characters that are neither letters nor numbers such as %$!~@; etc.). This also applies to:
  - systems that don't have the built-in capacity of locking out an account after a defined maximum threshold of unsuccessful login attempts have been exceeded; and
  - systems used to store encryption keys (i.e. private or secret key)
- There must be a secure, consistent method for processing and delivering a password reset.
- The password reset process must be controlled to ensure that only an authorised user can request a password reset, and that the account holder can be verified before the password reset is carried out.
- Users who have multiple failed access attempts must be locked out after a maximum of 6 sequential invalid password entry attempts.

5.5 Access to applications processing or storing BBC information must support SAML 2.0 as a minimum for exchange of authentication and authorisation, where integration is required with the BBC's SAML-compliant identity service.

5.6 The Third Party must ensure that multi-factor authentication (MFA) is used where possible, to protect privileged access accounts.

5.7 Where BBC Protected Information or above is being stored and/or processed or accessed, MFA must be used wherever available.

5.8 If you are handling BBC Restricted information you must consult BBC Information Security to agree specific controls to be applied. If you are unsure of the classification of your data, please contact BBC Information Security.

5.9 SMS should not be used for MFA where more secure methods of MFA are available.

5.10 The Third Party must ensure that the use of privileged utility programs that might be capable of overriding system and application controls, are restricted and tightly controlled.

5.11 The Third Party must ensure that remote support access to systems or applications that process or store BBC information is controlled via a secure gateway which implements the following controls:

- strong mutual authentication (e.g. MFA);
- access via a secure gateway (e.g. a firewall)
- remote support accounts are only enabled for the duration of the troubleshooting activity; and
- all troubleshooting activity is logged and reviewed.

5.12 Systems must implement onscreen password masking when a password is typed into a system (i.e. the system displays a row of asterisks rather than the actual passwords). See 6.5 for password encryption requirements.

5.13 Some systems and devices have pre-configured default passwords set by the manufacturer. All default passwords must be changed prior to the system/device being used to process or store BBC Information.

6. Cryptography

6.1 The Third Party must have a policy on the use of cryptographic controls to protect the confidentiality, authenticity and/or integrity of information.

6.2 Proprietary, private algorithms must not be used to protect BBC information unless tested and fully approved by BBC Information Security.

6.3 BBC Protected data must be encrypted at rest and in transit. BBC approved cryptographic algorithms can be found in Appendix B. These are provided for reference and represent a minimum standard, however other NIST approved algorithms may also be used.

6.4 If you are handling BBC Restricted information you must consult BBC Information Security to agree specific controls to be applied. If you are unsure, you must consult BBC Information Security.

6.5 All authentication information used to provide access to BBC information must be encrypted in transit. All such credentials must also:

- not be stored in plain text or in any reversible format;
- be salted with at least 64 bits of pseudorandom data; and
- be hashed in line with Appendix B.

6.6 Wireless infrastructure devices that are used to connect to a BBC network or provide access to BBC information must:

- use the WPA2 Standard;
- have Wi-Fi Protected Setup (WPS) disabled; and
- have controls in place to identify unauthorised wireless access points.

6.7 Where cryptographic keys are used to protect BBC information, the Third Party must have a policy on the use, protection and lifetime of the keys through their whole lifecycle. This should include as a minimum:

- generation of keys;
- issuing and obtaining public key certificates;
- distribution and activation of keys;
- storing of keys (including authorised access);
- changing or updating keys including when and how keys should be changed;
- dealing with compromised keys;
- revocation of keys (e.g. when they've been compromised or when a user leaves the organisation);
- recovering keys that are lost or corrupted;
- backing up or archiving keys;
- destruction of keys; and
- logging and auditing of key management-related activities.

7. Physical and environmental security

7.1 The Third Party must ensure that any equipment and facilities provided in relation to the Services are secured to prevent loss, damage, theft or compromise of BBC information. This includes:

- access control for entrances into the Third Party (or subcontractors') data centre (e.g. security guard, badge reader, electronic lock, court admissible CCTV) with logs recorded, reviewed and retained as necessary;
- physical access to premises restricted to those with a business need and the minimum access necessary to do their job;
- control of delivery and loading areas and all other points of access where unauthorised persons could enter the premises e.g. car parks with direct building access;

- emergency exit doors should be alarmed, monitored and tested in line with appropriate regional, national and international standards;
- power supplies and fire safety mechanisms undergo regular maintenance checks and comply with Health and Safety regulations; and
- intruder detection systems should be installed, monitored and tested in line with appropriate regional, national and international standards.

7.2 The Third Party must ensure that power and telecommunications cabling carrying BBC information or supporting information services in relation to the Services, are routed appropriately and protected where vulnerable to attack, interception or damage (e.g. periodic checks to identify unauthorised devices connected to the network).

7.3 The Third Party must implement and regularly test, uninterruptible power supplies (UPS) for critical infrastructure in relation to the Services.

7.4 The Third Party must ensure that a clear desk and clear screen policy is enforced in areas where BBC Protected and/or BBC Restricted information is stored. Documents containing such information must be kept secure when not in use. Devices should be locked when not in use and screens should not be visible to unauthorised personnel.

7.5 The Third Party must ensure that all equipment used to store BBC Protected and/or BBC Restricted information is disposed of or erased securely when no longer required. This includes:

- for paper copies using a confidential waste service or cross-cut shredder
  - minimum of the European DIN security level DIN 3 or equivalent for BBC Protected information,
  - minimum of DIN 4 or equivalent for BBC Protected - Commercially sensitive; BBC Protected – Legally privileged; BBC Protected – Personal or BBC Protected – Premium Content information; and
- sanitisation prior to, or during disposal of storage media using an ADISA (or equivalent) certified organisation; and
- a full audit trail must be recorded which includes the ability to track the individual assets being erased or destroyed, as well as the provision of an erasure or destruction certificate.
- For disposal of BBC Restricted information – contact BBC Information Security for specific advice.

8. Operations security

8.1 Procedures for operational activities in provision of the Services to the BBC must be documented, maintained and made available to anyone responsible for managing, administering or developing applications or systems used to process or store BBC information. This includes:

- the documenting of baseline platform builds;

- the removal/disabling of all unnecessary services from platforms; and
- all software installed on platforms being fully licensed and authorised for use.

8.2 Any changes to the organisation, business processes, systems or applications processing BBC information that affect information security must be controlled, documented and authorised through a formal process and agreed with BBC Information Security. Any such changes must be reviewed and tested to ensure that there is no adverse impact on services provided to the BBC or to the security of BBC information.

8.3 Capacity requirements must take into account the business criticality of the system. Procedures must require systems to be designed to cope with current and predicted information processing requirements. Regular monitoring and tuning must be applied to ensure that the required system performance is met and can be scaled accordingly.

8.4 Development, test and production facilities processing BBC information must be separated to reduce the risk of unauthorised access or changes to the operational environment or BBC information. The test environment should mirror the operational environment.

8.5 Controls must be in place to prevent, detect, eradicate and recover from malware threats. The Third Party must use all reasonable endeavours to detect hidden code or other methods that are designed to, or will have the effect of:

- destroying, altering, corrupting or facilitating the theft of any BBC information; or
- disabling or locking software or Third Party or BBC systems; or
- using unauthorised access methods for gaining access to BBC information or Third Party or BBC systems.

8.6 The Third Party must provide malware protection tools on all Third Party systems vulnerable to malware infection. Any such tool deployed should:

- be a current and supported version;
- be updated with definition or signature files on a daily basis as a minimum;
- provide real time on-access and on-demand scanning;
- scan all content entering and leaving the IT infrastructure processing BBC information;
- be able to disinfect, quarantine or delete malware;
- provide logging, alerts and reporting functionality; and
- be prevented from being disabled, inactivated or reconfigured by unauthorised users.

8.7 The Third Party must have processes in place to ensure the recovery from the loss or damage of BBC information or facilities used to process BBC information.

8.8 The Third Party must ensure that regular backups of all systems hosting BBC information are performed, and their restoration tested, dependant on the frequency of information change. A backup policy should be agreed with the BBC which includes as a minimum:

- the backing up of BBC information at scheduled intervals;
- validation of the backups;
- backup retention periods;
- backup type; and
- a testing schedule.

8.9 The Third Party must ensure that where backups are stored off-site, they are encrypted in line with this document and securely transported.

8.10 The Third Party must operate a real time-audit trail and log-monitoring process. Where required, this system should be able to interface with existing BBC logging and monitoring systems operated by the BBC and/or the BBC's technology services provider.

8.11 Security logging requirements must be considered, designed into systems, properly tested from the outset and discussed with BBC Information Security, to minimise the risk of disruption to BBC services.

8.12 Logging of user activities, exceptions, faults and information security-related events related to the processing of BBC information must be produced, kept securely, regularly reviewed, retained as agreed, protected against unauthorised access, alteration or deletions and backed-up in line with the agreed backup policy.

8.13 The logged information must include fields that are attributable to a single individual to ensure accountability and must be kept for an agreed time to assist with any possible investigations. Logs must be provided to BBC Information Security on request either as real-time or batch.

8.14 The clocks of all systems processing BBC information must be synchronised to an agreed accurate time source.

8.15 The Third Party must ensure that software installed on operational systems that store or process BBC information is tested, approved, up to date and in support.

8.16 Risk-based procedures for applying security patches and software updates to systems storing or processing BBC information must be formalised and implemented across the infrastructure.

8.17 Regular information must be obtained about technical vulnerabilities of systems being used to store or process BBC information and appropriate measures taken to address any associated risks.

8.18 A security risk assessment of the service being provided to the BBC must be completed by BBC Information Security or an approved delegate. The Third Party must ensure that any penetration testing indicated as necessary by the security risk assessment is completed before going live. The following testing should then occur during the Service lifecycle:

- System components, processes and software must be tested frequently to ensure that the security of BBC information is maintained.
- Where BBC Restricted information is being stored or processed, the Third Party must ensure that a full independent penetration test is carried out at least annually.
- The Third Party must ensure that a full independent penetration test is carried out at least annually when BBC Restricted or certain subsets of BBC Protected information are being stored or processed.
- Independent penetration testing must be carried out following:
  - any development of new builds
  - significant changes or major upgrades to infrastructure or
  - the introduction of new applications or upgrades to existing applications storing or processing BBC information.

In all cases, testing results and action plans are to be shared with BBC Information Security to ensure that the risks identified during testing have been mitigated to the satisfaction of the BBC and any residual risk accepted.

8.19 Rules governing the installation of software by users on operational systems storing or processing BBC information must be established and implemented. Users should only be granted the ability to install software where it is necessary for their role.

9. Communications security

9.1 The Third Party must maintain the appropriate confidentiality, integrity and availability of BBC information by:

- using secure network architecture and operations; and
- ensuring that networks and systems processing or storing BBC information are designed, built, monitored and managed according to industry standards, best practices and frameworks e.g. ISO27001, TOGAF, OWASP, ITIL etc. such that they enforce the required information security policy boundaries. These boundaries must prevent unauthorised access to systems and BBC systems or information by default.

9.2 The Third Party must ensure that anti-virus and firewall protection systems are implemented in relation to both internal and external traffic and ensure that:

- firewall platforms are hardened;
- penetration tests of firewall protected network connections are conducted annually by trained personnel;
- firewalls have real-time logging and alerting capabilities;
- firewall rules are regularly reviewed;
- intrusion detection/prevention systems are implemented where internet connections exist; and

- access lists are implemented on network routers to restrict access to sensitive internal networks or servers.

9.3 The Third Party must ensure that all IT systems used to provide Services to the BBC are protected from lateral movement of threats within the Third Party (and any relevant sub-contractors') network. The following should be considered:

- logical separation of device management ports/interfaces from user traffic;
- appropriate authentication controls; and
- the enablement of all available exploit mitigation controls in the operating system, installed applications and agents.

9.4 Where the processing or storing of BBC information takes place within a multi-tenanted environment, the Third Party must prevent the compromise of BBC information and provide separation between other consumers of services being provided.

10. System acquisition, development and maintenance

10.1 New information systems or enhancement to systems that store or process BBC information must have valid business requirements which must specify security controls to maintain or protect BBC information. The business requirements must be agreed by the BBC Service Manager and BBC Information Security, and must be subject to the Third Party's defined risk management process.

10.2 A policy document that outlines a secure process for the development of software and/or systems used in processing BBC information must be defined, maintained and applied.

10.3 Where the Third Party is developing systems and or applications as part of the provision of Services to the BBC, the Third Party must ensure that the following are built into the development lifecycle as a minimum:

- risk assessment/threat modelling process;
- secure design/architecture review;
- documented secure coding guidelines and industry good practice (e.g. OWASP) must be established, documented, maintained and applied. These should include user authentication techniques, secure session control, limiting the ability to enumerate, and data input validation and sanitisation;
- all components 'fail securely';
- all components run with least privilege;
- source code review; and
- security assessments which are performed in line with this document.

10.4 Development staff must be trained on secure coding principles and industry good practices. The training should be reviewed and kept up to date with new threats and vulnerabilities.

10.5 The Third Party must ensure that access to program source code is restricted and strictly controlled.

10.6 Restricted or Protected BBC information must not be passed unencrypted over public networks.

10.7 The Third Party shall ensure that all changes for information systems, upgrades and new software in relation to the services provided to the BBC have considered security control requirements based on identified risks. These changes should be tested both prior to, and after implementation to ensure that there is no adverse impact on operations or security. Any such changes should be managed in line with section 8.2.

10.8 Modifications to vendor-supplied software packages should be limited to necessary changes and must be strictly controlled, tested and documented.

10.9 Test data must be selected carefully, protected and controlled. Live BBC information that contains personal data or special categories of personal data information must not be used for development or test purposes.

10.10 Criteria for User Acceptance Testing (UAT) related to security must be agreed with BBC Information Security. The results of any such testing should be shared with BBC Information Security to ensure that BBC security requirements are met.

11. Offshoring

11.1 Any offshoring proposal by the third party or their subcontractor for delivery of services to the BBC must be subject to a full information security risk assessment and must be approved by BBC Information Security before it can go ahead.

11.2 BBC domain-wide administration privileges (e.g. Domain Admin, Enterprise Admin) must not be offshored without BBC Information Security approval.

12. Supplier and Partner relationships

12.1 The supplier or partner must provide full details of any subcontractor(s) that it intends to use in the provision of the Services to the BBC, before proceeding to use them. This includes as a minimum:

- company name;
- address
- geographic location of BBC information being accessed, stored or processed
- type of Services to be provided; and
- the volume, frequency and nature of BBC information to be used.

12.2 The Third Party must carry out an information security risk assessment and mitigate any identified risks prior to any subcontractor access to, processing or storing of BBC information. Unmitigated information security risks must be notified to the BBC.

12.3 The Third Party must ensure that subcontractor agreements contain security controls, service definitions, service requirements and delivery levels that are in line with the requirements set out in this document, and that these are implemented, operated and maintained at all times.

12.4 The Third Party must regularly monitor, review and audit subcontractors in line with the requirements set out in this document, where those subcontractors have access to, process or store BBC information.

12.5 The Third Party must manage changes to the provision of services by subcontractors ensuring that there is no adverse impact to the security of BBC information or services being provided to the BBC. Any changes that impact security must be notified to the BBC.

12.6 Exit requirements must be included in any agreement between the Third Party and the subcontractor. All access to BBC information must be revoked, and all BBC Information (including backups) must be deleted or destroyed in line with this document when no longer required, with appropriate evidence provided where required.

13. Information security incident management

13.1 The Third Party must ensure that security incident response responsibilities and procedures are established to ensure a quick, effective and orderly response to information security incidents.

13.2 Where the Third Party experiences or suspects that there may be an information security incident involving BBC information, BBC Information Systems and/or BBC network(s), the Third Party must:

- report it to the BBC as soon as possible after discovering the incident, and immediately (no later than 24 hours) if personal data is involved;
- undertake all reasonable steps to mitigate or contain the breach;
- promptly provide the BBC with a detailed written report setting out the details of, and reasons for the incident;
- provide the BBC, at no additional cost, with any assistance to restore the BBC Information, Systems and BBC Information Systems and any other assistance that may be required by the BBC;
- preserve evidence to include collection, retention and presentation of such evidence to BBC Information Security;
- promptly return to the BBC any copied or removed BBC Information;
- comply with all reasonable instructions from the BBC; and
- take remedial action to prevent reoccurrence of the same or similar security incident.

13.3 The Third Party must ensure that their employees and/or contractors report any observed or suspected security weaknesses in Systems or Services to their appointed point of contact. The Third Party must inform the BBC as soon as possible of any such weaknesses of which it becomes aware.

14. Information security aspects of business continuity management

14.1 A business continuity and disaster recovery plan that includes the continuation of information security in the event of an adverse situation, in relation to the provision of Services to the BBC must be established.

14.2 As a minimum, the plan must:

- set out how business operations will be restored following an interruption to or failure of business processes within an agreed time period, accepted by the BBC;
- set out how information security will be maintained;
- include arrangements to inform and engage the appropriate BBC personnel in its execution;
- be tested at regular intervals;
- be regularly reviewed and updated where necessary.

14.3 Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements for the provision of Services to the BBC including due consideration of potential infrastructural and geographic hazards.

15. Payment Card Industry Data Security Standard (PCI DSS)

15.1 Where financial transactions are (or becomes) a part of the Services, the Third Party must comply with the latest version of PCI DSS requirements, and provide annual evidence of PCI compliance through external certification or a self-assessment declaration.

16. Compliance

16.1 Legal, regulatory and/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 Data Protection, Freedom of Information, Privacy, Intellectual Property and proprietary software requirements.

16.2 BBC Information must be retained in line with defined retention periods and only for as long as is necessary for the purpose(s) for which it was collected.

16.3 The Third Party must implement processes to review their compliance with the requirements of this document. This process must be carried out annually as a minimum. If requested by the

BBC, the Third Party must give the BBC any necessary information so that the BBC can verify compliance.

16.4 To ensure compliance with BBC security requirements, the BBC (or a third party on behalf of the BBC) may carry out an information security assessment or audit. The Third Party must assist the BBC with the provision of any relevant documentation requested and provide access to all areas of the Site(s) as is necessary and when reasonably requested by the BBC.

16.5 If the Third Party has attained external validation or certification to any security industry standards e.g. ISO 27001, SSAE18, PCI DSS, the Third Party shall provide evidence of the relevant certification and any other supporting documentation e.g. Statement of Applicability, SOC 2/Type 2 reports upon request.

16.6 The Third Party must ensure that the storage and subsequent destruction of BBC Information is secure and in compliance with BBC instructions. All items of equipment used in the provision of the Services containing storage media must be checked by the Third Party to ensure that any BBC Information and licensed software has been removed or securely overwritten prior to secure deletion.

17. Exceptions Management

Where it is not possible to apply or enforce any part of this policy then a BBC Residual Risk Acceptance must be completed and returned to the BBC Information Security team. The BBC Information Security team will review the business justification, fully assess the risk and advise on any action to be taken before formally issuing any recommendations to the Information Risk Owner (IRO).

Once the BBC Information Security team receives confirmation that the risk has been signed off by the IRO, a BBC Information Security RRA ID will be assigned. Any proposed changes or extensions to the original RRA request must be reported to the BBC Information Security team so that the request can be reassessed.

Without a BBC Information Security RRA ID being issued, an RRA is not considered as approved.

18. Definitions

Term	Definition
Asset	Something that has value to an organisation including information, software, hardware, devices, services, people and intangibles (e.g. reputation).
At rest	Information stored on desktops, laptops, mobile devices (including removable media such as USB drives), in databases and on file servers as well as data that can be found in log files, application files and configuration files.
BBC information	Information in both logical or physical form. This includes stills and moving pictures, audio and video clips, and their associated metadata, as well as files.

BBC Materials	Any materials and/or devices supplied by the BBC to the Third Party or otherwise generated through the provision of the services under the agreement including but not limited to all devices, computer, hardware, computer and telecoms equipment, appliances, stationery, and any other materials, consumables, supplies or property of any kind.
BBC Network	Any electronic communications systems operated by the BBC.
In transit	Information moving from one location to another e.g. across the internet or through a private network.
Information Security Management System (ISMS)	A model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the protection of information assets.
Information System	The interrelated components that are used to collect, store and/or process information. This includes people, processes, systems, devices, hardware and software.
Least privilege	A principle restricting access to only the information and/or resources that are absolutely necessary to perform legitimate activities, and no more than this.
Multi-factor Authentication (MFA)	An extra level of security in addition to a username and password/passphrase such as a separate code sent to a mobile device, or biometric information such as a fingerprint.
Personal data	Any information relating to an identifiable, natural person who can be directly or indirectly identified by an identifier or whose identity can be pieced together. Examples include name, address, DOB, BBC staff number, location data or online IP Address.
Privileged utility program	A program that performs tasks related to the management or configuration of computer functions, resources, or files.
Public network	A network that anyone can connect to (e.g. the Internet).
Services	The services being provided by the Third Party to the BBC.
Sites	Any location used by the Third Party in providing the services including but not limited to the Third Party's site(s) and any other location where BBC information or materials are stored and/or processed.
Special categories of personal data	Personal data that is sensitive, namely race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometric data for the purpose of identification, health, sex life, and sexual orientation.
Subcontractor	Contractor appointed by the Third Party to provide all or part of the Services.
Third Party	Organisations (and their sub-contractors) that provide services to or partner with the BBC on a contractual basis.

19. Document control

Author	Vickie Greene		
Document Name	Third Party Information Security Requirements – BBC Data		
Version	1.3		
Source	BBC Information Security		
Document Owner(s)	Chief Information Security Officer		
Date	**Version**	**Author**	**Changes/Comments**
13/06/02019	1.0	Information Security Specialist (Policy)	First draft of revised version amalgamating all existing BBC infosec policy framework requirements into one document
03/09/2019	1.1	Information Security Specialist (Policy)	Updated following feedback from Head of Information Security (Governance)
22/11/2019	1.2	Information Security Specialist (Policy)	Updated following feedback from Infosec and wider BBC SME's
03/12/2019	1.3	Information Security Specialist (Policy)	Updated 5.3 and 5.5 following feedback from PRP.
17/12/2019	1.3	Information Security Specialist (Policy)	Approved by CISO
14/03/2023	1.4	Chris Gamble (Information Security Officer – Policy)	-Data Classifications in Appendix A updated to align with the updated Information Classification Policy -Clarification that suppliers need not adopt BBC Data (Section 4.3). -Control requirements in sections 5.7 and 7.5 have been adjusted to align with the updated Classification Policy and Handling Standard -A requirement to consult BBC InfoSec for specific advice if handling Restricted data has been added to sections 5.8, 6.4 and 7.5 -Clarification of when a penetration test is required (Section 8.18). -SHA-2 Hashing added to IPSec

			requirements in Appendix B to align with Encryption Standard

Appendix A – BBC information classification

If you are unsure of the classification of the information that you process or store on behalf of the BBC, you must consult your BBC contact for advice.

Public

This is information that is already publicly available or information that holds no confidentiality implications if disclosed.

Protected

BBC Protected information is defined as any information that does not fall under the definitions of BBC Restricted or BBC Public.

There is also a limited subset of BBC Protected information that need specific handling measures to meet regulatory and BBC business requirements. This subset of information should still be managed within the BBC Protected tier but there may be additional security controls that need to be in place to protect it:

- **Protected – Commercially sensitive**

  Commercial or market sensitive information which may be severely damaging to the BBC or to a commercial partner if it was improperly accessed or disclosed.

- **Protected – Legally privileged**

  Confidential communications between BBC lawyers and the person(s) they are advising, (this may be the BBC itself).

- **Protected – Personal**

  Particularly sensitive information relating to an identifiable individual, where inappropriate access could have damaging consequences. For example, as part of an investigation, criminal convictions, special categories of personal data, children's personal data, staff personal data and on-air talent personal data.

- **Protected – Premium Content**

  Content relating to any brand with a significant fan-base either in the UK or globally, or a significant investment and/or return is classified as Premium Content. Examples of Premium Content are Doctor Who, Sherlock and Top Gear. These titles are subject to specific Premium Content security controls. Responsibility for deciding which content should be subject to these controls sits with the Global Editorial Director and the Chief Brands Officer.

Restricted

BBC Restricted information is defined as:

- Journalistic sources who need to remain anonymous.
- Information that could result in a threat to life.
- Information that could prejudice national security.

Appendix B – Encryption protocols and algorithms

- Where symmetric encryption is required to protect BBC information at rest, the minimum level required is a key size of 256-bit, a block size of 128-bit and 10 rounds.

- Where encryption of BBC information in transit is required, the following minimum levels apply:

  - **Symmetric stream encryption**: a key size of at least 256-bit.
  - **Symmetric block encryption:** a key size of at least 256-bit, a block size of 128-bits, 10 rounds.
  - **Asymmetric encryption:** a key size of at least 2048-bit RSA or equivalent strength.
  - **Hypertext Transfer Protocol Secure (HTTPS):** Transport Layer Security (TLS) 1.2.
  - **Secure Shell (SSH):** SSH-2.
  - **Secure File Transfer Protocol (SFTP)**: version 3 or above must be used. File Transfer Protocol (FTP) and File Transfer Protocol Secure (FTPS) are not permitted.
  - **Internet Protocol Security (IPSEC)**: for secure data connections between devices communicating over Internet Protocol (IP) networks using the minimum of AES-256 encryption and SHA-2 hashing.

- Where a cryptographic hash function is required to protect BBC information, the minimum level is SHA-256.