BBC Third Party Information Security Requirements – BBC Data

Last reviewed: 14/03/2023

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.

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.

- 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-ed

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

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

			requirements in Appendix B to align with Encryption Standard

Appendix A – BBC information classification

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.