# BBC Third Party Information Security Requirements – non-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 provide services or information to the BBC but do not process or store BBC information.

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

## Contents


1. Introduction ..... 4
2. Information security governance, policy and standards ..... 4
3. Human resources security ..... 5
4. Access control ..... 5
5. Data handling ..... 5
6. Physical and environmental security ..... 5
7. Information security incident management ..... 6
8. Payment Card Industry Data Security Standard (PCI DSS) ..... 6
9. Compliance ..... 6
10. Supplier relationships ..... 7
11. Exceptions Management ..... 7
12. Document control ..... 8

# BBC Third Party Information Security Requirements – non BBC data

## 1. Introduction

The BBC relies on the integrity and availability of information and systems in order to deliver its services as stated in its Charter, and to enable subsidiaries to fulfil their commercial objectives.

It is essential that the BBC maintains the trust of all its stakeholders and remains compliant with relevant legal and regulatory requirements. This means ensuring that third parties who provide services to the BBC have an appropriate approach to information security.

### 1.1 Scope

This document sets out the minimum security requirements expected of third parties who provide services or information to the BBC, but do not process or store BBC information. This includes (but is not limited to):

- systems integrators providing a system or solution to be managed by the BBC;
- support, consultancy services to BBC systems;
- provision of data feeds;
- management of events associated with the BBC;
- panels of research participants; or
- panels of competition judging participants

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.

## 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. NIST, ISO27001).

**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.

**2.3** The Third Party must ensure that its information security policies are published, kept up to date and effectively communicated to all relevant staff.

## 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** 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.

**3.3** Information security awareness, training and education must be provided to all third party employees (including freelancers/contractors) as relevant to their role.

## 4. Access control

**4.1** Access to information or systems being used to provide Services to the BBC must only be granted to those personnel who need to perform such Services.

**4.2** Permissions and access must be removed when a person providing Services to the BBC no longer performs that role. Where the BBC provides access then the Third Party must notify the BBC as soon as it becomes known that the person should no longer have access.

## 5. Data handling

**5.1** The Third Party must maintain safeguards against the accidental, deliberate or unauthorised disclosure, access, manipulation, alteration, destruction, corruption, damage, loss or misuse of information issued to the BBC as part of the Services being provided.

**5.2** Use of encryption must be in line with security industry best practice.

## 6. Physical and environmental security

**6.1** The Third Party must ensure that any equipment and facilities are secured to prevent loss, damage, theft or compromise of assets used or provided as part of the Services. This includes:

- access control at entrances, exits and other points of access where unauthorised persons could enter the premises; and
- power supplies and cabling.

## 7. Information security incident management

**7.1** 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.

**7.2** Where the Third Party experiences or suspects that there may be an information security incident involving the Services being provided to the BBC, 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.

## 8. Payment Card Industry Data Security Standard (PCI DSS)

**8.1** 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 to the BBC of PCI compliance through external certification or a self-assessment declaration.

## 9. Compliance

**9.1** Legal, regulatory and/or contractual requirements must be complied with. In particular this includes, but is not limited to, compliance with Data Protection, Freedom of Information, Privacy, Intellectual Property and proprietary software requirements.

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

## 10. Supplier relationships

**10.1** Where the Third Party uses subcontractors in the provision of the Services to the BBC, they must regularly monitor, review and audit the subcontractors to ensure that they have appropriate security measures in place.

## 11. 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.**

## 12. Document control

| | | | |
|---|---|---|---|
| **Author** | Vickie Greene | | |
| **Document Name** | Third Party Information Security Requirements | | |
| **Version** | 1.0 | | |
| **Source** | BBC Information Security | | |
| **Document Owner(s)** | Chief Information Security Officer | | |
| **Date** | **Version** | **Author** | **Changes/Comments** |
| 07/10/2019 | 0.1 | Information Security Specialist (Policy) | First draft for review |
| 12/01/2021 | 1.0 | Information Security Specialist (Policy) | Approved |
| 14/03/2023 | 1.0 | Chris Gamble (Information Security Officer – Policy) | Reviewed – No Changes |