Corporate Information Security Policy

Overview	Sets out the high-level controls that the BBC will put in place to protect BBC staff, audiences and information.
Audience	Anyone who has access to BBC Information Systems however they are employed or under a term of contract, including third parties.
Owner	Head of Information Security
Contacts	Information Security Policy & Compliance Manager Information.Security @bbc.co.uk
Updated	24/11/2014
Other related information	Acceptable Use of Information Systems Policy Business Continuity Management Data Protection Handbook Identity & Access Control Policy Information Security Policy Framework Security Codes of Practice Security Review & Compliance Policy

Contents

1 Introduction

The BBC handles a lot of information and relies on the availability, integrity and confidentiality of that information to deliver services.

The BBC approach to information security is based on risk. This means that the BBC is able to maintain its creativity in offering new products and services, whilst at the same time protecting against any threats that the BBC or its audience may face.

This policy is part of the Information Security Policy Framework.

If you have any questions about this policy please contact BBC Information Security.

1.1 Purpose

This policy sets out the high-level controls that the BBC will put in place to protect BBC staff, audiences and information by ensuring that:

- information risks are managed to a level that is acceptable to the BBC;
- security incidents are minimised and dealt with effectively as and when they do happen; and
- the BBC complies with any legislative, regulatory and contractual obligations relating to the security of information (e.g. the Data Protection Act).

1.2 Audience

This policy applies to anyone who has access to BBC Information Systems however they are employed or under a term of contract, including third parties.

1.3 Scope

All people, processes and technology that transmit, store or process BBC information.

2 Information Security Principles

1. It is the responsibility of everyone working for the BBC to maintain the security of the information, devices and systems that we use.
2. Appropriate security measures will be used to protect the public's trust in the BBC.
3. No one person or event should be allowed to have a negative impact on the BBCs activities.
4. The BBC will always try to use information security good practice and comply with relevant legal and regulatory requirements.
5. Information security will be based upon a balanced risk management approach meaning that we will apply appropriate levels of protection and control to BBC information.
6. BBC Information Security will take into account the BBC's business and creative needs when applying security safeguards.

7. New products and services are a core part of the BBC. BBC Information Security will take into account their creative value when assessing the security risk they may pose.

3 Human resources security

3.1 Prior to employment: All BBC employees will:

- have a background check in line with any legal, regulatory or BBC policy requirements; and
- understand what their information security responsibilities are before starting their employment with the BBC.

3.2 During employment: All BBC employees (including contractors) will:

- apply security in line with BBC information security policies and procedures;
- receive regular information security awareness and training to help them achieve this. Where necessary this will include job role specific training; and
- be aware that any breach of security may result in a formal disciplinary procedure.

3.3 Termination or change of employment: Any termination or change of employment at the BBC will be securely managed using formal processes and procedures.

4 Information risk management

4.1 Risk management: The BBC will protect its Information Assets by identifying, assessing and treating risks in line with BBC Information Risk Management policies and processes.

5 Information asset management

5.1 Responsibility for assets: Information Assets will be assigned an Information Asset Owner who will be responsible for the maintenance and security of their assets.

5.2 Asset classification & handling: Agreed procedures will be followed to ensure that Information Assets are classified and handled securely.

6 Identity and access management

6.1 Managed identities and access: Access to information, applications and systems will be appropriately controlled and restricted. Access will be provided based on business security requirements and be appropriate to a user's responsibilities.

7 Operational security

7.1 Operational security architecture: The BBC will provide a framework for applying standard information security controls to new and existing systems. This will provide consistent and comprehensive security functionality across the entire BBC infrastructure.

8 Change management

8.1 Changes to the technical environment: All changes to the BBC technical environment or any third-party connecting environment will be managed by a formally documented change management process. Security risk assessments will be carried out on all applicable changes.

9 Information systems development management

9.1 Systems development methodology: All systems development activity will follow an approved Systems Development Lifecycle (SDLC) methodology that ensures security is considered at all stages of the development lifecycle.

9.2 Separation of environments and duties: Development and production environments will be isolated at physical, logical and administrative levels. Segregation of duties will be enforced between development and release management functions.

10 Information security incident management

10.1 Incident management: Formal information security incident procedures will be maintained. These will enable the BBC to be prepared for, identify, contain, eradicate, recover and learn from incidents in a controlled and managed way.

10.2 Employee responsibility: It is the responsibility of anyone working for, with and on behalf of the BBC, to report all suspected or actual information security incidents as detailed in the Acceptable Use of Information Systems Policy. Any suspected breaches of personal information will be reported to Information Policy & Compliance.

11 Information back-up

11.1 Information back-up: The strategy for backing up BBC Information will include security requirements that align with legal and regulatory requirements for data retention, business continuity plans and support the BBC's risk appetite.

12 Business continuity and disaster recovery

12.1 Business continuity management: Business impact assessments, business continuity and disaster recovery plans will be produced for all critical information, applications, systems and networks in line with the Business Continuity Policy.

13 Physical and environmental security

13.1 Security in and around the BBC buildings: Appropriate controls will be applied when selecting, constructing, renovating or operating any BBC location. Processes and procedures will be used to ensure a secure environment for both BBC employees and Information Systems. These can be found in the Security Codes of Practice.

14 Compliance monitoring

14.1 Compliance with information security policies: Procedures will be put in place to manage compliance with information security policies, related standards, procedures, processes and safeguards.

15 Exceptions

15.1 Exceptions process: Where it is not possible to apply or enforce any part of this policy then a BBC Dispensation Request must be completed and returned to BBC Information Security. BBC Information Security will review the business justification and advise on the risks involved. Policy exceptions will only be issued when the Data Owner has signed off on the identified risks.

16 Roles and Responsibilities

Information Security Advisory Forum (ISAF)	Reviewing this policy
Information Security Compliance Board (ISCB)	Reviewing and approving this policy.
Information Security Governance and Compliance	Maintaining this policy, monitoring for compliance and providing advice and guidance on its implementation.
Divisional managers and BBC Partners	Understanding which policy statements are relevant and implementing them within their areas of responsibility.

17 Definitions & References

17.1 Definitions

Availability	Ensuring information is accessible and usable by authorised users when it is needed.
Confidentiality	Ensuring information is only made available to authorised user(s) and not disclosed in an unauthorised way.
Information Asset	1. A set of data which can be reasonably grouped together where the contents, media, location, access controls, classification and subsequent impact to the BBC for loss, breach or destruction (temporary or permanent) are the same; or 2. A single piece of data where it is unique in any of the criteria mentioned in point 1 above and cannot be sensibly grouped with other data.
Information security	Ensuring the integrity, availability and confidentiality of information.
Information security incident	An event or series of events that cause the reduction or compromise of information security, resulting in a negative impact on business operations.
Information Systems	Systems, devices, services (e.g. Internet, email, and telephony), applications or equipment that are used to store, transmit or process information in an electronic or physical form.
Integrity	Ensuring that information is complete and accurate and has not been tampered with, altered or damaged in an unauthorised way.
Risk Appetite	A shared understanding of the overall level of risk which an organisation and the senior team is prepared to carry.

17.2 References

Acceptable Use of Information Systems Policy
Business Continuity Management
Data Protection Handbook
Identity & Access Control Policy
Information Security Policy Framework
Security Codes of Practice
Security Review & Compliance Policy

18 Document Control

Author	BBC Information Security		
Document Name	Corporate Information Security Policy		
Version	1.2		
Source	BBC Information Security		
Policy Owner(s)	Head of Information Security		
Date	Version	Author	Changes/Comments
11/04/2013	1.0	AR	Final Version approved by ISCB
27/10/2014	1.1	VG	Minor rewording and updated formatting for Gateway policy project agreed at ISCB on 27/10/2014.
24/11/2014	1.2	VG	Updated 15.1 to reference the dispensation process