



## FORCE INFORMATION SECURITY POLICY

### 1 POLICY STATEMENT

- 1.1 The purpose of this policy is to protect British Transport Police (BTP) information assets, whether paper-based or electronic from all threats, whether internal, external, deliberate or accidental.
- 1.2 The implementation of this policy demonstrates the commitment of BTP in complying with the requirement of the Data Protection Act 1998 Principle 7 and the Association of Chief Police Officer (Scotland) Community Security Policy (ACPO(S) CSP).

### 2 OVERVIEW

- 2.1 This replaces the existing Force Information Security Policy and sets out BTP's aims in relation to information security.
- 2.2 The general public has a right to expect that all members of BTP will, when utilising information in connection with BTP business, ensure:
  - (a) The confidentiality of all BTP information, whether electronic or paper-based, and that only authorised users have access.
  - (b) The integrity of information by ensuring its accuracy and completeness.
  - (c) The availability of information systems and information therein whenever required by authorised users.
  - (d) That information is disclosed only to those authorised to receive it.
  - (e) That information disclosed is used only for Police purposes.
  - (f) That regulatory and legislative requirements are met.
  - (g) That information security training is available to all staff.



- 2.3 The loss, damage, wrongful destruction or wrongful disclosure of information could result in substantial costs to BTP as well as a reduction in public confidence.
- 2.4 Responsibility for information security in BTP ultimately rests with the Chief Constable. The responsibility for the monitoring and management of this policy has been devolved to the Corporate Assurance Group (CAG) under the chair of the Finance Director.
- 2.5 Supporting this overarching policy is a range of detailed policies and Standard Operating Procedures (SOPs) that must also be adhered to.

### 3 TERMS AND DEFINITIONS

- 3.1 An **Information System** is any facility or practice that is used to store or process business information in any form.
- 3.2 An **Information Asset** is information that has value to BTP.
- 3.3 The term **Employee(s)** refers to all BTP officers and staff.
- 3.4 The term **Contractor(s)** includes the main supplier of goods or services, their servants, agents and subcontractors.
- 3.5 The term **User(s)** applies to any Employee or Contractor or other authorised people who use or access BTP information.



- 3.6 The term **Security Incident** is any suspected failure in information security, namely:
- Accidental or deliberate unauthorised destruction of information
  - Accidental or deliberate unauthorised modification of information
  - Accidental or deliberate unauthorised disclosure of information
  - Deliberate and unauthorised unavailability of systems
  - Unauthorised access to systems or information
  - Misuse of data and theft of assets
  - Any contravention of Information Security or Vetting Policies and associated Standard Operating Procedures
  - Any other event which affects security of information.

#### 4 SECURITY REQUIREMENTS

- 4.1 All security incidents whether actual or suspected must be reported to the Professional Standards Department through line managers and in accordance with the Force Information Security Manual (Annex B).
- 4.2 BTP will provide cost and risk effective protection through adequate and efficient safeguards and countermeasures, against all nature of threats to its information assets.
- 4.3 Protection will be through an appropriate combination of personnel, physical, procedural, technical and management security controls outlined in the Force Information Security Manual.
- 4.4 Enhanced security protection will provided for information assets that are identified as being key to BTP business.



4.5 The CAG shall be responsible for all policies with respect to how information is gathered, stored and processed as part of any information system whether manual or computerised.

## **5 ROLES AND RESPONSIBILITIES**

5.1 The DCC is the Senior Information Risk Owner (SIRO), who is the representative at COG level and understands the strategic business goals of the organisation and how these may be impacted by failure of information systems. The SIRO also ensures that management of information risks are weighed alongside the management of the other risks facing the organisations such as financial, legal and operational risks.

5.2 The Chief Information Officer is responsible for developing, producing, maintaining and delivering the business strategic plans for Information Management and Technology for BTP, within budget and to agreed timescales, and ensuring that all Information and Technology work streams support the strategic aims of BTP.

5.3 Area Commanders and Heads of Department are responsible for implementing the policy within their areas and for adherence by their staff.

5.4 The Force Information Security Officer has direct responsibility for maintaining the policy, providing guidance on its implementation and ensuring compliance with policies, standards and procedures.

5.5 The Regional Information Security Officers provide guidance and assistance to Area Commanders and Heads of Department.



- 5.6 System Owners are responsible for System Administrators, and ensure compliance with policies and procedures in respect of individual systems within their remit.
- 5.7 System Administrators provide day-to-day support to the System Owner in pursuit of their information security responsibilities.
- 5.8 Line Managers should be aware of the Information Security Policy and their individual responsibilities as well as those of their staff; to ensure compliance within their area of responsibility.
- 5.9 All BTP staff are Users, and it is each of their responsibility to adhere to this policy; to abide by any SOPs as outlined in system accreditation documentation; to abide by the conditions of employment by maintaining the confidentiality, integrity and availability of information; and to use BTP information assets for policing purposes only.

## **6 APPLICABLE DATE, MONITORING AND REVIEW**

- 6.1 This policy applies from 11 November 2008 and applies to all employees and contractors.
- 6.2 This policy will be reviewed in response to any significant changes in legislation or business purpose. There will be a three-year review of this policy to ensure that BTP continues to follow best practice.
- 6.3 Continuous monitoring of this policy will be undertaken by Information Security staff as part of the departmental audit plan.



## 7 OWNERSHIP

- 7.1 This policy is owned by the Deputy Chief Constable.
- 7.2 Any questions and comments related to this policy should be directed to the Force Information Security Officer.

## 8 ASSOCIATED DOCUMENTS AND POLICIES

When reading this document, please also refer to:

- Force Information Security Manual
- Protective Marking SOP
- Identity Card SOP
- Laptop SOP
- MFD SOP
- Password SOP
- Portable Data Storage Devices SOP
- Remote Access SOP
- Security of Buildings, Rooms and Containers SOP
- Handling Secret and above Material SOP
- Destruction of Protectively Marked Assets SOP
- Home Working SOP
- Change Control SOP
- BTP Vetting Policy and SOP