BRITISH TRANSPORT POLICE

BRITISH TRANSPORT POLICE	**POLICY**

POLICY INFORMATION	
Title	Access Control Policy
Version	V2.0

POLICY OWNERSHIP	
Policy Sponsor	Director Strategy & Change
Policy Owner	Head of Information Management
Policy Author	Force Information Security Officer

British Transport Police welcome comments and suggestions from the public and staff about the contents and implementation of this policy. If you have any queries relating to this policy please write to: **Information Governance Unit British Transport Police 2nd Floor, 3 Callaghan Square Cardiff, CF10 5BT** or email: **FOI@btp.pnn.police.uk**

Purpose of the Policy

This policy addresses the risk of unauthorised access to, and consequent misuse of, national policing and British Transport Police (BTP) classified information assets. The objective is to meet the specific Home Office and legal requirements to deliver effective and auditable controls over who can access national policy systems and BTP technology systems, and when that access may or not be granted. The policy provides the foundation stone of any rule or role-based authentication and authorisation control based on user access.

Who does this policy apply to

This policy refers to those employees (both permanent and fixed term) who at any time may be joining BTP for the first time (starters), moving to a new position with the Force (movers) or exiting the Force after a period of employment (leavers). This policy will also apply to temporary staff, volunteers, and third parties who require access to technology systems or information assets.

This policy is applicable in England, Scotland and Wales.

Principles

BTP provides its employees with secure access to BTP technology systems, BTP information assets and national police IT systems to conduct their roles effectively. It is an overarching requirement that the access rights of employees are maintained in an accurate and timely fashion. This requirement is fundamental to data governance attributes such as quality, auditability, accuracy and security. The responsibility for ensuring employees maintain appropriate access to systems, data and assets, in accordance with their role, lies on a day-to-day basis with line managers, but ultimately with the Information Asset Owners (IAO) and Senior Information Risk Owner (SIRO).

Monitoring and Review

This policy will be reviewed every 3 years and in response to any significant changes in legislation or business purpose.

BRITISH TRANSPORT POLICE

Associated Policies/Documents

BTP Information Risk Management Strategy

HMG Security Police Network

The Cabinet Office PSN Code of Connection

Cabinet Office/CESG End User Device Strategy: Security Framework and Controls

Data Protection Act

Computer Misuse Act

ISO/IEC 27001 Information Security Management Systems