BRITISH TRANSPORT POLICE

BRITISH TRANSPORT POLICE	**POLICY**

POLICY INFORMATION	
Title	Data Loss Prevention Policy
Version	V2.0

POLICY OWNERSHIP	
Policy Sponsor	Director of Capability and Resources
Policy Owner	Head of Information Management
Policy Author	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**

BRITISH TRANSPORT POLICE

Purpose of the Policy

This policy addresses the risk of intentional and unintentional leakage of national policing and British Transport Police (BTP) classified information assets. This policy does not address risks of equipment failure, business continuity or disaster recovery; these are covered by business continuity or disaster recovery policies.

Who does this policy apply to

This policy applies to Technology Department staff tasked with developing, maintaining and implementing IT processes and procedures.

The stakeholders for this Data Loss Prevention Policy comprise:

- Director of Capability and Resources
- Head of Technology
- Information Security Manager
- Departmental Heads and Area Commanders
- Line managers
- Any other 3rd party with which BTP has a current data handling agreement in place before the data sharing takes place.

Principles

BTP policy regarding data loss prevention are as outline below.

- BTP documents containing classified information will be marked with an embedded security classification to facilitate technical measures within boundary controls to prevent data loss and indicate to information users its classification and handling requirements.
- The following boundary controls will implement technical measures to prevent data loss:
  - Email attachment filters (outgoing)
  - Internet/web traffic (outgoing)

- Data at rest on portable computers will be protected from theft/loss by use of assured encryption.
- Data at rest on portable data storage devices will be protected from theft/loss by use of assured encryption.
- Boundary controls shall be cognisant of the levels of classification that are/are not appropriate for each egress path. For example, some classifications may be permitted for transmission over secure email systems, or for upload to secure websites within the PSN-P network.
- Boundary controls will block content that obfuscates electronic security classifications by encryption (e.g. zipped files).

Monitoring and Review

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

Associated Policies/Documents

Data Loss Prevention Guidance

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

CESG Good Practice Guide No. 8 – Protecting External Connections to the Internet

CESG Good Practice Guide No. 13 – Protective Monitoring for HMG ICT Systems

CESG Good Practice Guide No. 30 – Assurance of ICT Systems and Services