Government Security Classification Scheme (Policy)

OFFICIAL

Publication Scheme Y/N	Policy section can be published on Force Website Procedure should be withheld
Department of Origin	Corporate Support & Development (CSD)
Policy Holder	Head of CSD
Author	Information Assurance Coordinator (CSD)
Related Information	Data Protection Act Freedom of Information Act Government Security Classifications Human Rights Act 1998
Date Approved at SMB	21/03/2018
This Version	V.1
Date of Next Review	21/03/2022

March 2018

Policy

Statement

In October 2015 the National Police Chiefs' Council (NPCC) agreed that all forces would adopt the new Government Security Classification Policy/Scheme (GSCS) thus replacing the previously used Government Protective Marking Scheme (GPMS).
https://www.gov.uk/government/publications/government-security-classifications

This policy provides guidance to staff on how to handle information using the new Government Security Classifications (GSC).
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

This policy does not need to be applied retrospectively to existing information, but applies to any new information within the organisation. However any classification should be updated when documentation/assets are subject to review.

The change has been referred to as the Government Security Classification Policy and the Government Security Classification Scheme. They are the same thing and will be referred to as Government Security Classifications (GSC) throughout this document.

Aims

The aim of this Policy is to assist all personnel to understand and use GSC in accordance with the NPCC decision, which has been adopted by Merseyside Police.

All information assets must be classified in line with the GSC. The term 'Information asset' includes any information which has value to policing purposes and wider police business which are held in any format (hard copy or electronic) E.g. evidence documents, operational orders, briefing sheets, plans, maps, photographs, audio and video recordings.

In order to know how to adequately protect information and data, it is important that all staff understand how to classify the information they use according to the sensitivity of that data. All classifications and associated protective measures should be based on the information contained within the document and the principle of *'Need to know.'*

The marking applied to the information asset must be based on its' content and the possible effects that could arise from any form of compromise, for example:

- breach of confidentiality through the information being disclosed or revealed to those without a 'need to know',
- information being exposed to, alteration, or unauthorized change such that it may not be able to be relied upon
- it not being available to those who need it

Applying a classification to an asset indicates to others the appropriate level of handling and controls required to appropriately protect it against such compromises.

GSC has three **primary** classifications:

- OFFICIAL
- SECRET
- TOP SECRET

Where a classification has been considered but not applied, police information assets are deemed to be '***OFFICIAL'*** by default and treated as such.

As the majority of information processed by Merseyside Police personnel will be categorised as 'OFFICIAL' or 'OFFICIAL – Sensitive' by definitions, the aims of this policy are to:

- Safeguard the organisation's information.
- Protect the personal data of data subjects
- Protect the organisation from potential legal liabilities and its' reputation
- Ensure all individuals have an understanding of the classifications and are provided information as to their personal responsibility
- Establish the minimum security standards necessary when working with OFFICIAL and OFFICIAL - Sensitive information.

The Categories of 'Secret' and 'Top Secret' will be used comparatively rarely by the Police Service but this policy also provides guidance for their use.

Objectives

A broad objective is to ensure all individuals using police information select the most appropriate protective marking in order to protect information whilst making it suitably available for those who have a lawful basis and necessity to process it and for users of information to understand their personal responsibilities when processing information.

More specific associated objectives are to:

a) Protect personal data

b) Reduce operational risk by safeguarding confidential and sensitive information

c) Protect the organisation's reputation and safeguard it from legal liabilities

d) Reduce the volume of security breaches

e) Reinforce the professional standards of behaviour expected of all Police information users.

f) Comply with the requirements of Information Management: Authorised Professional Practice

Application and Scope

This policy applies to all users who access or process Merseyside Police information.

Failure to comply with this policy may lead to a breach of information security and may lead to disciplinary action. Any suggestion that an individual is in breach of the standards required will be thoroughly investigated and they may be liable to disciplinary action.

The Chief Officer lead for this policy is the Deputy Chief Constable.

Outcome Evaluation

The Information Assurance Coordinator (IAC) will monitor compliance with this policy.

The Professional Standards Department (PSD) Anti-Corruption Unit (ACU) is responsible for ensuring use of ICT systems and the processing of force information is audited and monitored. Relevant data will include the number of cases investigated by the ACU and complaints/referrals to Professional Standards Department (PSD) on associated protective marking issues.

The IAC will oversee the reporting of security breaches and monitor them.

Outcome

Merseyside Police will become consistent with protective marking used by HMG and an increasing proportion of the Public Sector thereby enhancing the security of the processing of information and being able to demonstrate ‘Adequacy’ in this area of Information Security by protecting data