SOUTH WALES POLICE
FORCE POLICIES & PROCEDURES

POLICY IDENTIFICATION PAGE

This policy has been drafted in accordance with the principles of human rights legislation.

Public disclosure is approved unless otherwise indicated and justified.

Policy title: Force Information Security Policy (FISP)

Policy reference number: 282

Issue number: 06

Underlying procedures

Governance, Risk Management and Compliance
Government Protective Marking Scheme (GPMS)
Personnel Security
Information Security Assurance
Physical Security
Business Continuity Management (BCM)
E-mail and Internet Use
Mobile Computing
Mobile Phones
Remote Working
Access Control
Acceptable Use

Chief Officer: ACC Specialist Operations

Policy written by: Force Information Security Office

Department responsible: Corporate Information Management & Technology

Policy Lead: Force Information Security Officer

Links to other policies:

HMG Security Policy Framework (SPF)

Policy implementation (First published) date: 01/08/03

Policy review date: April 2012

SOUTH WALES POLICE
FORCE POLICIES & PROCEDURES

INTRODUCTION

PRINCIPLES AND AIM OF POLICY

- Enable the delivery of core operational policing by providing appropriate and consistent protection for the information assets of South Wales Police.
- Comply with statutory requirements and meet ACPO/ACPOS expectations of the Police Service to manage information securely.
- To ensure that South Wales Police meet the Policing Pledge with respect to securing information assets.
- Enable South Wales Police to meet the required standard of information security to access critical national systems.

ORIGINS/BACKGROUND INFORMATION

INTRODUCTION

The Chief officers of South Wales Police recognise that information, including the supporting processes, systems and networks, is a valuable asset to South Wales Police (SWP).

Responsibility for determining Information Assurance policy within SWP, implementing that policy and acting as the regulatory authority is invested in the Information Security Board (ISB). The ISB is chaired by the ACC Specialist Operations who also acts as the Senior Information Risk Owner (SIRO) and reports directly to ACPO.

In line with the above, this policy is owned and maintained by the Information Security Board (ISB).

PURPOSE

The FISP details the strategy for the securing of information processes throughout SWP and forms a framework for other subordinate policies including:

- Individual System Security Policies
- Risk Management and Accreditation Document Sets (RMADS)
- Codes of Connection to National Systems and Services
- Business Continuity Plans,
- Security Operating Procedures (SyOps)

GOALS AND OBJECTIVES

Information exists in many forms and can be written on paper, stored electronically, transmitted by post or electronic means, shown on films or spoken in conversation. The Chief Constable supports the need for appropriate safeguards and the effective management of all information processes, and is committed to helping protect all SWP information assets from identifiable threats.

These threats can be internal or external, deliberate or accidental. By implementing this policy, SWP are ensuring Confidentiality, Integrity, Availability and Non-repudiation of information.

This policy provides the necessary controls to mitigate against the consequences of SWP being exposed to unacceptable business risks. These risks include the safety of operational Police Personnel, the compromise of sensitive operations and ultimately loss of public confidence.

Information Assurance will be achieved by undertaking risk assessments and implementing appropriate controls, covering policies and procedures for physical security, personnel security and technical security.

SWP shall ensure that information systems and processes comply will all applicable legislation regulatory requirements which include:

- The Data Protection Act 1998
- The Human Rights Act 1998
- The Computer Misuse Act 1990
- The Official Secrets Act 1911-1989
- The Copyright, Designs and Patents Act 1988
- The Regulation of Investigatory Powers Act 2000
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

The Information Management Unit is responsible for ensuring that SWP information and processing complies with the principles contained in Data Protection and Freedom of Information legislation. The Force Information Security Office (FISO) is responsible for ensuring that the necessary measures are taken to protect the confidentiality, integrity and availability of all SWP information assets.

Any conflicts or obligations placed on the Force by DP or FOI legislation shall be referred to ACC Specialist Operations for decision.

THREAT

Generic threats to information security emanate from many sources including Foreign Intelligence Services (FIS), subversive organisations, terrorist and criminal groups, investigative journalists, disaffected personnel, members of the public and natural disasters including fire and flood. These threats may manifest themselves via the unauthorised activities of personnel (due to inadequate awareness training, disinterest, disaffection or coercion), the interception of communications (electronic and manual), physical disruption (including criminal damage and theft) and unauthorised access to information assets by both

members of the public and internal personnel.

In conjunction with other Government agencies, regular assessments will be undertaken to identify specific threats to SWP systems and information. These will be authorised by the ISB and conducted by the Force Information Security Office. The FISO will report the result of these audits to the ISB for action.

APPLICABILITY

This policy is mandated for all officers and staff in SWP, including contractors and agency staff and third parties who work on SWP information or process it on behalf of SWP.

SCOPE

The FISP encompasses all manual and electronic information processing systems and provides a mechanism by which SWP can develop, implement and measure effective information security management systems (ISMS). This will provide SWP with the strategies and countermeasures to identify threats and vulnerabilities.

The FISP applies to all information assets owned by SWP whether or not such information is being stored or processed on SWP premises and should be considered as the primary reference document when developing security operating procedures (SyOps) for information systems.

RESPONSIBILITIES

Each Department within SWP will implement and maintain strategies enabling information to be managed and secured therefore ensuring, its Confidentiality, Integrity, Availability and Non-repudiation.

When required to do so, SWP must demonstrate compliance with the ACPO Community Security Policy (CSP) using the NPIA supplied CSP Compliance Matrix. This is submitted to NPIA annually, by the Force Information Security Office (FISO).

COMPLIANCE STANDARDS

SWP has adopted a number of Government and Industry compliance standards that provide the foundation and framework for applying, implementing, managing and measuring effective information assurance controls to common criteria.

Compliance with these standards is necessary to provide assurance to ACPO/ACPOS Pan Governmental Departments and other community members that the risk to community information and interconnected community systems can be shown to have been mitigated to acceptable levels.

Compliance with the standards outlined in this policy also allows SWP to reach the required standard to be eligible for access to key national systems such as the Police National Computer (PNC) and the Police National Database (PND).

The following standards have been adopted by SWP and together form the foundations upon which this policy is based and shall be used by SWP as benchmark requirements:

- Cabinet Office HMG Security Policy Framework, which includes HMG Information Assurance Standards and Memoranda (published on behalf of HMG by CESG);
- ISO/IEC 27001 Information Technology – Security techniques – Specification for an Information Security Management System;
- Statutory Code of Practice on the Management of Police Information 2005;
- ACPO Guidance on the Management of Police Information (MoPI) 2006;
- Electronic Information Processing Security Notices (S(E)N) issued by the Cabinet Office Security Policy Division;
- HMG Information Assurance Maturity Model and Assessment Framework;
- The ACPO National Vetting Policy for the Police Community;

COMPLIANCE REQUIREMENTS

In order to comply with the requirements of the ACPO Community Security Policy (CSP), SWP must:

- Undertake a risk assessment and accreditation process approved at local SIRO level for systems with connections to the CJX and other national information systems.
- Submit Risk Management and Accreditation Sets (RMADS) for SWP domains connecting to national systems to the National Accreditor for Police Systems (NAPS).
- Complete and submit on an annual basis a CSP Compliance return as determined by PIAB, via the National Accreditor for Police Systems (NAPS). This return is currently the CSP Compliance Matrix.
- Provide evidence of independent auditing in accordance with any audit requirements issued by PIAB.
- Immediately report via POLWarp or the NPIA Information Assurance Team any incident that has the potential to compromise the security of national systems.

The Force Information Security Office (FISO) will ensure that SWP comply with the above compliance requirements.

SPECIFIC GUIDANCE – Governance, Risk Management and Compliance

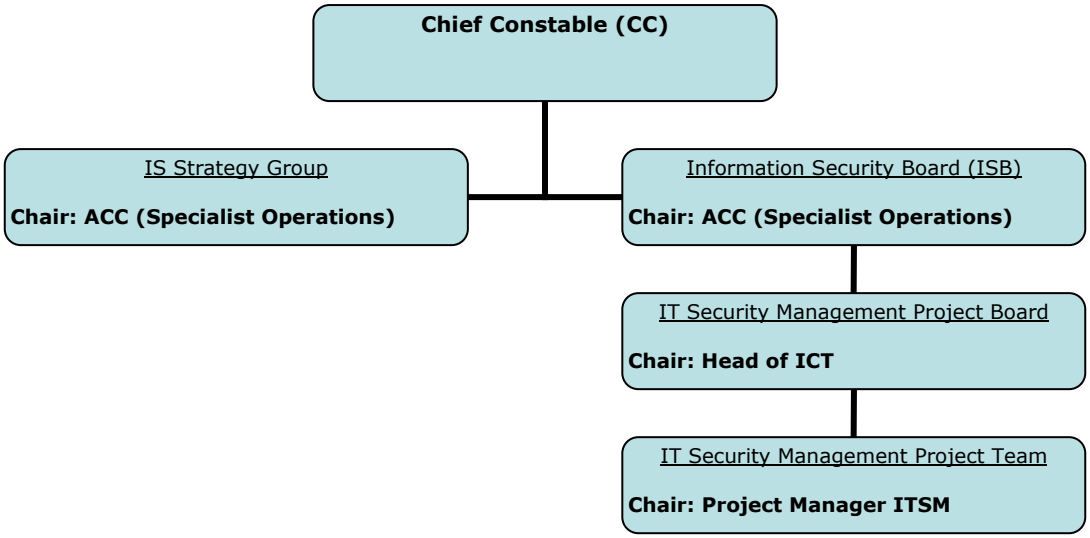
PROCEDURAL HEALTH AND SAFETY CONSIDERATIONS
NONE

SPECIFIC PROCEDURES

SWP Information Security Governance Structure

A management structure with senior management leadership has been established to approve information security policy, assign security roles and co-ordinate the implementation of information security across the organisation.

This is outlined in the diagram below:



With this in mind the SWP Chief Officers have set up a Management framework, consisting of the Information System (IS) Strategy Group and the Information Security Board (ISB) which feeds into it. The IS Strategy Group has been set up to provide the following:

- Ownership of the Integrated Information Strategy;
- An authority to spend against a defined corporate IS budget;
- Delegated COIG decision making for all IS decisions;
- Sanctioning the commencement of corporate change projects and allocation of spend against those projects through approval of a defined business case.
- Providing sponsorship for corporate projects and providing appropriate management of those projects particularly in respect of project prioritisation and benefit realisation;
- Focusing on the vision of a single system and removal of tactical solutions

The chair of the IS Strategy Group is ACC (Specialist Operations), as of this time of writing this includes representatives from all ownership groups and chairs of all systems change boards where not already attending as part of 2nd Tier.

The Information Security Board (ISB) provides a forum that includes members of all the key departments which are seen as having a contribution to the overall Information Security of SWP.

The ISB is chaired by the ACC (Specialist Operations) and includes the Heads of ICT, Human Resources, Estates, Facilities, Professional Standards, Training and Corporate Information Management (CIMD).

The ISB oversees and directs the work of a project called the 'IT Security Management' (ITSM) Project. The aim of this project is two fold, to bring the IT network infrastructure up to a suitable standard of security and to develop a more workable IT security management structure. This project is expected to run for around two years and once completed, IT security management will become business as usual. The ITSM Project Board is chaired by the Head of ICT and includes relevant ICT and Information Management personnel. The ITSM Project Team is chaired by the ITSM Project Manager and includes tactical level ICT and a representative from the Force Information Security office (FISO).

SWP Chief Officers have also appointed Force Information Security Officers to provide specialist information security advise to departments and users. The Force Information Security Officers jointly fulfil the role of the Departmental Security Officer (DSO) for SWP, as outlined in the HMG Security Policy Framework (SPF). The Force Information Security Office (FISO) can be contacted on x20-954 and x20-682.

The FISO maintains contact with external security specialists to keep up with industry trends, monitor standards and assessment methods and provide suitable liaison points when dealing with security incidents.

SWP Chief Officers have determined that a multi-disciplined approach to information security, involving the co-operation and collaboration of managers, users, administrators, application designers, auditors and security staff is the best approach to managing information security for the organisation.

Roles and Responsibilities

Whilst security is a collective responsibility for all staff and contractors, within SWP ultimate responsibility for security rests with the Chief Constable. The Chief Constable delegates the day to oversight of this to the Senior Information Risk Owner (SIRO), which sits within the portfolio of the ACC (Specialist Operations).

The Force Information Security Officer(s) (FISO) has been designated to fill the role of the Departmental Security Officer (DSO) for SWP and is responsible for ensuring that the Senior Information Risk Owner (SIRO) is kept up to date with any risks, which may affect the Force.

Risk Management

SWP has adopted the HMG IS1 standard for Risk Assessment and Management and the FISO is responsible for its day to day management. All departments within SWP are required to 1) identify their information assets and those responsible for them 2) understand the vulnerability and likelihood of attack from various threats, 3) value them in terms of the impact from loss or failure of confidentiality, integrity and availability and 4) assign a proportionate level of protection to mitigate, and / or recover from, the potential loss or failure of those assets. Departments should see this as a continuous cycle of assessing and re-evaluating risk.

SWP will adopt the HM Treasury Orange Book on Risk Management for a broad approach to principles and concepts, however, within the disciplines of information assurance and counter-terrorism protective security there are detailed methods of risk assessment that must be adopted.

Assurance

Assurance covers three areas, self-assessment central reporting and audit and review. All three of these must work together to provide a robust level of assurance across SWP. Each of these three areas are discussed below:

Self-Assessment

a) It is a mandatory requirement laid out in the HMG Security Policy Framework – to make the Force Information Security Policy (FISP) available internally. With this in mind SWP have posted the Force Information Security Policy on the Force Intranet and therefore it is now available to anyone who needs it;
b) The ISB routinely task the FISO with audits and inspections to ensure compliance with the FISP and all aspects of protective security and then to report back to the ISB their findings;

Central Reporting

It is a mandatory requirement within HMG Security Policy Framework to submit an annual Force Statement on Internal Control to the Cabinet Office Security Policy Division via the National Police Improvement Agency (NPIA), this report must include the following:

a) Details of any changes to key individuals responsible for security matters, such as the appointment of a new FISO, which must be reported immediately.
b) Significant department risks and mitigations that have implications for protective security nationally within the police service.
c) All significant security incidents (those involving serious criminal activity, damage to National Security, serious reputation damage, data losses or leaks).

This reporting is normally handled by the Force Information Security Office (FISO) under direction of the ISB.

Audit and Review

As mentioned above, the ISB tasks the FISO to carry out internal reviews of

security arrangements as they judge necessary. This also includes the annual IT Health Check carried out in compliance of the CJX Code of Connection. NPIA require SWP to produce a Security Compliance statement annually detailing the information security position of the Force.

Culture, Training and Professionalism

To improve the professional culture and to develop a positive attitude toward security, the ISB has taken steps to ensure that Information Security is seen as an integral part of and a key enabler to effective business. In line with this, all new starters undergo an induction course which covers the individual's responsibility to comply with the Data Protection Act, the Freedom of Information Act and the Force Information Security Policy (FISP).

Also each member of staff, must annually complete the online GPMS Training on FIS. Information Security is now a part of the annual EPDR.

INDIVIDUAL ROLES AND RESPONSIBILITIES

Chief Constable

It is the Chief Constable responsibility to ensure compliance with the MoPI code of practice and implementation of the guidance. The Chief Constable is the Owner of IMS and is the Data Controller. The Chief Constable will ensure the existence of appropriate security measures for police information systems and that these are audited in accordance with ACPO/ACPO[S] (2006) Information Systems Community Security Policy v3. It is the Chief Constable responsibility to ensure appropriate resourcing of identified roles and functions. Staff are trained in compliance with NPIA Training and Delivery Strategy.

Senior Information Risk Owner (SIRO)

Must be of ACPO or equivalent level and have strategic ownership of risk. This role is currently in the portfolio of ACC (Specialist Operations). The SIRO as chair of the ISB also owns all of the RMADS for ICT Systems and is responsible for ensuring that they are kept up to date and for authorising new user access to these systems.

Assistant Chief Constable (Specialist Operations)

Overseas the functions of a number of departments including Corporate Information and Technology, which incorporates ICT and Corporate Information Management. The ACC Specialist Operations also acts as SWP Senior Information Risk Owner (SIRO).

Assistant Director Corporate Information and Technology

The Assistant Director CI&T is responsible for overseeing the day to day management of CI&T and updating the ACC Specialist Operations on corporate risk.

Head of Corporate Information Management

The Head of Corporate Information Management overseas all functions for management of police information. The Head of Corporate Information Management is also responsible for keeping the Assistant Director CI&T informed of corporate and information risk.

Business Process Owners

Ensure that ICT systems support the implementation of business process relevant to their area keeping in mind relevant legislation and best practice.

Force Information Manager

The Force Information Manager is responsible for the day to day management of the Information Management Unit, which comprises of the Force Information Compliance Unit, and the Force Information Security Office. The Force Information Manager keeps the Head of Corporate Information Management up to date with any risks or issues regarding Data Protection, Freedom of Information and Information Security.

Force Information Compliance Manager

The Force Data Protection Manager is responsible for managing the Chief Constables statutory obligations in respect of the Data Protection Act 1998 and also ensures management of the forces obligations under the Freedom of Information Act (FoIA) 2000.

Force Information Security Officer(s)

Ensures compliance with relevant guidance and legislation. Able to implement security consistent with local and national requirements. Acts as the Departmental Security Officer (DSO) for SWP as outlined in the HMG Security Policy Framework (SPF).

Provide advice and guidance on security education, training and good practice.

Information Technology Security Officer (ITSO)

Provide advice and guidance on security practice and delivery within the ICT department. This role is currently handled by one of the FISO's.

Monitor information security across ICT.

Ensure compliance with all relevant legislation and guidance, in regard to ICT systems and implement correct controls in line with the Force Information Security Policy (FISP) and good practice. Acts as the point of contact within ICT on Information Security Issues.

Force Records Manager

Ensures compliance with the FoIA. Develop and maintains standards for records

management to secure a coordinated approach.

Senior System Owner/System Owners

Responsibilities as outlined in MoPI. Ensuring risk management processes are carried out within the programme or project. Processes in place for managing and controlling number and type of systems in force and delegation of ownership. Ensure that SIRO is aware of residual risks.

Disclosure Manager

Responsibility for CRB checks. Investigates through an approved structure; assessing the relevance of the information and suitability for disclosure accordingly.

Force Accreditor

Responsible for assessing the residual risk affecting the Force's information systems. Responsible for accrediting information systems on behalf of SIRO, or raising the risk if it is deemed to great to the SIRO for sign off. In line with HMG Policy, the Force Accreditor must have direct access to the SIRO.

Crypto Custodian

Ensures that all cryptographic material coming into the Force is handled in line with government procedures and guidelines and then ensure that the cryptographic material is distributed promptly and securely in line with CESG Guidance.

SOUTH WALES POLICE
FORCE POLICIES & PROCEDURES

SPECIFIC GUIDANCE – Government Protective Marking Scheme (GPMS)

PROCEDURAL HEALTH AND SAFETY CONSIDERATIONS
NONE

SPECIFIC PROCEDURES

Introduction

The Government Protective Marking Scheme (GPMS) is the Government administrative system to ensure that access to information assets is correctly managed and safeguarded to an agreed level throughout their lifecycle, including creation, storage, transmission and destruction. The system is designed to support SWP business and meet the requirements of relevant legislation, international standards and international agreements.

The UK Police Service adopted the GPMS in 2002. Within SWP it is a mandatory requirement for all staff to be familiar with the GPMS and to have done the online GPMS training available on Kallidas. This training must be undertaken on an annual basis to comply with Force Policy. Any breach of this policy in regard to the GPMS may result in disciplinary action being taken.

Legal Requirements

SWP have a legal requirement to adhere to the following legislation:

- ***The Official Secrets Act 1989*** – this act makes no mention of the GPMS, but does specify the categories of interests to which damage must, or must potentially be caused by the unauthorised disclosure. These are 1) Security and Intelligence, 2) Defence, 3) International relations, 4) Foreign confidences, 5) Crime, 6) Special Investigation powers.

- ***The Data Protection Act 1998*** – this legislation requires appropriate management structure and control. Proper application of the GPMS will also ensure that protectively marked information is appropriately safeguarded and that requirements of the DPA are met. Whilst the DPA makes no reference to the GPMS, protective marking may be a helpful indicator that an exemption applies. The presence, or absence of a protective marking is not in itself a deciding factor as to whether or not information should be released in response to a subject access request, but it may nevertheless provide some initial guidance as to whether and which exemption applies.

- ***Freedom of Information Act 2000*** – gives any person the right to request and be provided with information held by public authorities, although exemptions apply to specific information as defined by the Act. Whilst the FOIA makes no reference to the GPMS, protective marking may be a helpful indicator that an exemption applies. The presence, or

absence of a protective marking is not in itself a deciding factor as to whether or not information should be released in response to a FoI request, but it may nevertheless provide some initial guidance as to whether and which exemption applies.

The 'Need to Know' Principle

The effective use of information is a key priority for SWP. Access to sensitive information assets will be required for the efficient management of SWP business. However, access must only be granted to those who have a business need and the appropriate personnel security vetting. This 'need to know' principle is fundamental to the security of all protectively marked SWP assets. Casual access to protectively marked assets is never acceptable. If there is any doubt about giving access to sensitive assets individuals should consult their managers or FISO before doing so.

International Security Standards

The GPMS is designed to meet the principles of the international standard on Information Security Management Systems (ISO/IEC 27000 series). This standard represents good practice to which this policy is aligned.

The Government Protective Marking Scheme (GPMS)

The Government Protective Marking Scheme comprises six markings. In descending order of sensitivity they are: **TOP SECRET**, **SECRET**, **CONFIDENTIAL**, **RESTRICTED** and **PROTECT**. The term **NOT PROTECTIVELY MARKED** must be used for material that is identified as suitable for public consumption or for publication.

These markings are applied to any government assets, although they are most often commonly applied to information held electronically or in paper documents. The methodology used to assess these principles within information systems is expressed in Business Impact levels.

The Business Impact levels (commonly called Impact levels) are shown below:

- Impact Level 0 – **NOT PROTECTIVELY MARKED**
- Impact Levels 1 & 2 – **PROTECT** - [with suitable descriptor, e.g. STAFF]
- Impact Level 3 – **RESTRICTED**
- Impact Level 4 – **CONFIDENTIAL**
- Impact Level 5 – **SECRET**
- Impact Level 6 – **TOP SECRET**

Universal Controls

All staff must comply with the following mandatory controls in regard to protectively marking material:

a) Access is granted on a genuine 'need to know' basis;
b) Assets must be clearly and conspicuously marked. Where this is not practical (for example the asset is a building, computer etc) staff must still have the appropriate personnel security controls and be made aware

of the protection and controls required;

c) Only the originator or designated owner can protectively mark an asset. Any change to the protective marking requires the originator or designated owner's permission. If they cannot be traced, a marking may be changed, but only by consensus with other key recipients;
d) Assets sent overseas (including to UK posts) must be protected as indicated by the originator's marking and in accordance with any international agreement. Particular care must be taken to protect assets from foreign Freedom of Information legislation by use of national prefixes and caveats or special handling instructions;
e) No official record, held on any media, can be destroyed unless it has been formally reviewed for historical interest under the provisions of the Public Records Act;
f) A file, or group of protectively marked documents or assets, must carry the protective marking of the highest marked document or asset contained within it (e.g. a file containing CONFIDENTIAL and RESTRICTED material must be marked CONFIDENTIAL);

Applying the correct protective marking

The originator or nominated owner of an information asset is responsible for applying the correct protective marking. When protectively marking a document, a damage or 'harm test' is conducted to consider the likely impact if the asset were to be compromised and to help determine the correct level of marking required. The 'harm test' should be done by assessing the information asset against the criteria for each protective marking and then applying the one that fits the best.

The following points must be considered when applying a protective marking:

- Applying too high a protective marking can inhibit access, lead to unnecessary and expensive controls and impair the efficiency of an organisations business;
- Applying too low a protective marking may lead to damaging consequences and compromise of the information asset;
- The compromise of aggregated or accumulated information of the same protective marking is likely to have a higher impact (particularly in relation to personnel date). Generally this will not result in a higher protective marking but may require additional handling arrangements;
- The sensitivity of an information asset may change over time and it may be necessary to reclassify information assets. If a document is being re-classified or the marking changed, the file should also be changed to reflect the highest marking within its contents;

For more information on the GPMS, please see the GPMS leaflet available on the Force Intranet or from your FISO.

Information Security Breaches

If a member of staff becomes aware of any breaches of the GPMS, then they must inform their line manager and the Force Information Security Officer(s) at the earliest opportunity. There is a link on the Force Intranet under Tools which contains the online form for reporting security breaches.

INDIVIDUAL ROLES AND RESPONSIBILITIES

BCU Commanders/Department Heads

Are responsible for making sure that the GPMS is adhered to within their department and that every member of staff is properly trained in using it.

Line Managers

Are responsible for making sure that all the staff in their unit is compliant with the GPMS and that any document which leaves their office is properly marked.

The Line Manager is also responsible for ensuring that their staff follow the online GPMS training curriculum and that they undergo the annual refresher training.

Any breaches of this policy must be reported directly to the FISO.

Users

It is the user's responsibility to make sure that they mark properly every document which they produce, so that sensitive information is given the correct protection.

It is everyone's responsibility to ensure that all documents they create are protectively marked (Refer GPMS on Connect).

Information that has been protectively marked must be handled and disposed of in the correct manner. For more information please see the above information or contact the Information Security Office.

SPECIFIC GUIDANCE – Personnel Security

PROCEDURAL HEALTH AND SAFETY CONSIDERATIONS
NONE

SPECIFIC PROCEDURES

Purpose

The purpose of personnel security is to provide a level of assurance as to the trustworthiness, integrity and reliability of all SWP employees, contractors and temporary staff. As a minimum requirement all staff is subject to controls known as the Baseline Personnel Security Standard (BPSS). For more sensitive posts there are a range of security controls referred to as "National Security Vetting (NSV)": these are specifically designed to ensure that such posts are filled by individuals who are unlikely to be susceptible, for whatever reason or motive, to influence or pressure which might cause them to abuse their position.

Risk Management

SWP have employed a risk management approach to Personnel Security in conformity with the National ACPO Vetting Policy, seeking to reduce the risk of damage, loss or compromise of SWP information assets. For this reason SWP have implemented a Force Vetting Unit, which are responsible for ensuring that SWP comply with ACPO Policy and best practice. The Force currently has an interim Force Vetting Policy as the current National Vetting Policy is being updated. For more information please contact the Force Vetting Unit.

Baseline Personnel Security Standard (BPSS)

Baseline Personnel Security Standard (BPSS) is the recognised standard for pre-employment screening. It forms the foundation for National Security Vetting and seeks to address identity fraud, illegal working and deception generally. The BPSS comprises verification of four main elements 1) identity, 2) employment history, 3) nationality and immigration status and 4) unspent criminal records. BPSS allows regular access to UK RESTRICTED and UK CONFIDENTIAL information assets and occasional or supervised access to UK SECRET information assets, provided they have a 'need to know'.

National Security Vetting

There are three levels of National Security Vetting: Counter-Terrorist Check (CTC), Security Check (SC) and Developed Vetting (DV). Vetting is required for those who have unescorted access to sites to work in close proximity to individuals assessed to be at risk of terrorist attack, who have access to information assets which may be of interest to terrorists or have frequent access to SECRET and / or TOP SECRET information assets. National Security Vetting

involves a degree of intrusion into an individual's private life and must only be applied in accordance with HMG statement policy and the Force Vetting Policy.

Access to Force Systems

It is a requirement as part of the Accreditation program within SWP, to set the requirements for personnel vetting for users and administrators of the system. If the system has been protectively marked as RESTRICTED or CONFIDENTIAL then users should be vetted to Baseline Standard (BS). If the system is marked as SECRET then the user should be SC Cleared. For systems marked as TOP SECRET, Deep Vetting (DV) is a mandatory requirement.

The personnel security or vetting requirements are different for ICT staff as they routinely have access to large quantities of protectively marked information, for this reason it is a mandatory requirement for all ICT staff to be SC cleared as outlined in the FISP section, Governance, Risk and Compliance. This is also a mandatory requirement for all staff, third party suppliers and contractors regardless of how they access the system.

INDIVIDUAL ROLES AND RESPONSIBILITIES

Senior Management Responsibilities

Managers at responsible for ensuring that:

a. All individuals working in posts involving access to, or knowledge or custody of, sensitive government assets, have appropriate levels of assurance and security clearance and;
b. When security clearances are reviewed, or when post holders change, line managers are consulted as to whether or not there is a continuing need for the posts to attract levels of assurance or security clearances and if so, the controls required;

It is important to remember that security clearance does not, on its own provide a guarantee of an individual's integrity and trustworthiness. Since individuals and their circumstances change, a security clearance is only as good as the background records and other investigations on which it is based at the time the process is carried out. It is important that personnel security continues after the initial security clearance is approved and that any new information or concerns that may affect the reliability of a person are brought promptly to the attention of the Vetting Manager. This is achieved through a combination of aftercare and security clearance review procedures. For more information on Personnel vetting review periods please see the Force Vetting policy <LINK>.

Line Management Responsibilities

Effective personnel security is dependant on the support of line managers. Line Mangers are responsible for the following:

a. Maintaining the standards of security expected and;

b. Briefing post holders about the protection of assets and processes under their control.

In particular Line Managers are responsible for ensuring that any potential difficulties or conflicts of interest among staff are identified and reported as soon as possible to the Force Information Security Office (FISO).

Human Resources Responsibilities

Effective personnel security controls also require close cooperation between HR and the Force Information Security Office to ensure that:

a. HR will be informed on a regular basis of issues likely to be of security significance through the medium of the Information Security Board (ISB). These issues may have impact on recruitment procedures and policies, it is the responsibility of HR senior management to ensure that any such issues are dealt with as quickly as possible to ensure the continued security of the organisation;
b. HR Information likely to be of security significance is routinely passed to the FISO to ensure that no relevant information is overlooked and;

The FISO must be consulted about an individual with CTC, SC or DV clearance, for whom security concerns have been raised, before the individual is transferred to another CTC, SC or DV post.

The Force Vetting Unit

The Force Vetting Unit is responsible for ensuring that the Force vetting process adheres to the ACPO National Vetting Policy as well as fulfilling the Force's obligations on 'aftercare'.

SOUTH WALES POLICE
FORCE POLICIES & PROCEDURES

SPECIFIC GUIDANCE – Information Security and Assurance

PROCEDURAL HEALTH AND SAFETY CONSIDERATIONS
NONE

SPECIFIC PROCEDURES

Managing Information Risk

Information is a key asset to SWP and its correct handling is vital to the delivery of public services and to the integrity of SWP. In striking the right balance between sharing and protecting data, SWP must manage business impacts and risks associated with Confidentiality, Integrity and Availability (CI &A) of all information. Information Assurance (IA) is the confidence that information systems will protect the information they carry and will function as they need to, when they need to and only under the control of legitimate authorised users.

Roles and Responsibilities

The Chief Constable has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. This responsibility is supported by the Senior Information Risk Owner (SIRO), which currently sits in the portfolio of ACC Specialist Operations and the day-to-day duties has been delegated to the Force Information Security Officer (FISO).

The information security functions which support the protection of SWP Information Systems are risk management, accreditation, standards and compliance. The HMG Security Policy Framework requires that SWP must:

- **Conduct an annual technical risk assessment** (using HMG IA Standard No.1) for all SWP ICT Project and Programmes and when there is a significant change to a risk component to existing SWP information systems. The assessment and the risk management decisions made must be recorded in the Risk Management and Accreditation Document Set (RMADS), using HMG IA Standard No 2 – "Risk Management and Accreditation of Information Systems.
- **Use Business Impact Levels (ILs)** – in conjunction with the GPMS, use Business Impact Levels to assess and identify the impacts to the business through the loss of Confidentiality, Integrity and/or Availability of data and ICT systems should risks be realised.
- **Submit an annual statement of Internal Control (SIC)** – SWP must submit an annual SIC to NPIA which has been signed off by the Senior Information Risk Owner (SIRO).
- **A Designated Senior Information Risk Owner (SIRO)**: must be a board level individual responsible for managing Force information risks, including maintaining and reviewing an information risk register. Within

SWP the SIRO is the ACC Specialist Operations.

- **A Designated Information Technology Security Officer (ITSO)**: responsible for the security of information in electronic form. This role is currently carried out by the Force Information Security Officer (FISO).
- **A Designated Communications Security Officer (ComSO)**: responsible for the cryptographic material. This role is currently carried out by the Force Information Security Officer (FISO).
- **Designated Asset Owners**: senior named individuals responsible for each identified information asset. This is currently carried out for the Force by the Information System Strategy Board (ISSB), chaired by the SIRO.

It is advised (by HMG Security Policy Framework (SPF)) that the ITSO reports directly to the DSO on information security matters. Where this is not the case, there should be clear mechanisms to ensure that IT Security is considered as part of the overall approach to protective security. SWP have combined the DSO. ITSO and ComSO roles into the Force Information Security Officer (FISO) role. Through the current IT Security Management Project, these areas are addressed.

Accreditation and Audit

SWP have implemented an accreditation regime in line with HMG IA Standard No. 2, with the FISO as the lead for this. All new information systems are accredited before going live and are then reviewed annually thereafter.

The following are mandatory requirements from the HMG Security Policy Framework for all Police Forces:

- ICT Systems that process protectively marked data must be accredited using HMG IA Standard No. 2 – "Risk Management and Accreditation of Information Systems" prior to going 'live'. The project manager is responsible for ensuring that the Risk Management Document Set (RMADS) is completed and handed to the Local Accreditor (FISO). The accreditation status must be reviewed at least annually to judge whether material changes have occurred which could alter the original accreditation decision;
- Regular compliance checks must be carried out by the accreditor, as documented in the RMADS;
- A forensic readiness policy that will maximise the ability to preserve and analyse data generated by an ICT system, that may be required for legal and management purposes;
- All ICT systems must have suitable identification and authentication controls to manage the risk of unauthorised access, enable auditing and the correct management of user accounts;
- SWP must follow the requirements of any codes of connection (such as CJX and xCJX) policies to which they are signatories. Codes of connection should cover the following technical policies:
    - Patching policy, covering all ICT Systems including operating systems and applications, to reduce the risk from known vulnerabilities;
    - Policy to manage risks posed by al forms of malicious software (Malware) including viruses, spy-ware and phishing etc;

- Boundary security devices – (e.g. firewalls) must be installed on all systems with a connection to untrusted networks, such as the internet;
- Content checking/blocking policy;
- Lockdown policy to restrict unnecessary services and ensure that no user has more privileges (access functionality) than required;

Where these are not covered by codes of connection, separate policies covering these areas must be established.

Cryptography and Communications

The HMG Security Policy Framework (SPF) has the following mandatory requirement regarding the management of Cryptography:

- SWP must comply with HMG IA Standard No.4 – "Communications and cryptography (Parts 1 – 3) for the protection of protectively marked material. Paying particular attention to the circumstances when encryption is required, the requirement to only use CESG approved solutions, the control mechanisms for cryptographic items, and the requirements for specified levels of personnel security clearance for individuals handling cryptographic items; The ComSO is currently one of the roles carried out by the FISO and ensure that these guidelines are met;
- SWP must follow specific Government procedures to manage the risk posed by eavesdropping and electro-magnetic emanations;

Remote Working/Mobile media

Home or remote working introduces a new set of vulnerabilities and risks with offsite and portable ICT devices and media (e.g. laptops, PDA's, phones, memory sticks, and external drives). HMG Standards and guidelines must be used for connecting to public (insecure) ICT systems such as the Internet. All departments should also, when handling personnel data, avoid where possible the use of mobile media.

SWP have implemented a Remote Working, which all staff that use remote technology are required to adhere too.

Procurement

SWP must ensure that security requirements are specified in ICT contracts and all new ICT contracts handling personnel data must adhere to the Office of Government Commerce (OGC) ICT model terms and conditions. All ICT equipment must be purchased through SWP ICT, unless specifically approved by FISO.

Reporting Incidents

If any member of staff becomes aware of an information security breach then they must inform their line manager and the FISO at the earliest opportunity. There is also a facility to report information security incidents online, using FIS, under the tools subsection.

Secure Disposal

Staff must ensure that all media used for storing or processing protectively marked or otherwise sensitive information must be disposed of or sanitised in accordance with HMG IA Standard No. 5 – Secure Sanitisation of Protectively Marked or Sensitive Information.

All offices within SWP premises are provided with white bags, specifically for sensitive waste. These white bags are suitable for RESTRICTED and CONFIDENTIAL material. RESTRICTED documents can be put into the sack as is, but CONFIDENTIAL documents should be suitably shredded using an appropriate cross-shredder.

Any magnetic media should be disposed of securely via ICT's contract with Reisswolf, who will securely dispose of the media.

Personnel and Physical Security

Personnel and physical security are integral elements in mitigating information risk. Whilst standards outlined in HMG Security Policy No. 3 and HMG Security Policy Framework No. 5 deal with these, it should be noted that ICT and cryptographic posts must be specifically evaluated to assess the level of security clearance required. Moreover the physical security of ICT hardware and infrastructures must be specifically addressed as recommended by the HMG Security Policy Framework:

- Departments and Agencies must ensure that ICT users with higher privilege and/or potentially wide access (e.g. system administrators, architects, programmers etc.), or those with responsibility for ICT security, must be subject to evaluation for National Security Clearances appropriate to the protective marking of the information processed;
- Departments and agencies must ensure that all locations where information and system assets (including cryptographic items) are kept must have an appropriate level of physical security as set out in this framework;

Because of the above SWP have evaluated both the ICT (who have administrative access across multiple systems), including third party contractors and suppliers who have access to SWP Systems, either physically or remotely and Crypto Custodian posts and have determined that SC clearance is sufficient.

Education, training and awareness

SWP based on the requirements in the HMG Security Policy Framework outlined below:

- Departments and agencies must ensure that all users of ICT systems are familiar with the security operating procedures governing their use, receive appropriate security training and are aware of local processes for reporting issues of security concern. They must further ensure that staff who manage and maintain the secure configuration of ICT systems and those with access to information assets, are appropriately trained, are aware of incident reporting, and the minimum standards relating to the

handling of protectively marked data;

The project manager and system owner is responsible for ensuring that all the users of a particular system are made properly aware of their responsibilities in regard to the information security of the system they are using. This must be included as part of the standard training on the system prior to the system going 'live'.

Business Continuity and Disaster Recovery Planning

HMG Security Policy mandates that:

- Departments and agencies must ensure that all locations where information and system assets (including cryptographic items) are kept must have appropriate Business Continuity and Disaster Recovery Plans;

For this reason SWP have implemented a number of initiatives to develop Business Continuity and Disaster Recovery Plans and have tested some of these in a mock incident called Operation Taliesin. There is also an ICT Project called TIM which has one of its deliverables, a basic DR infrastructure for a small number of critical ICT systems.

INDIVIDUAL ROLES AND RESPONSIBILITIES

Chief Constable

The Chief Constable has overall (ultimate) responsibility for ensuring that information risks are assessed and mitigated to an acceptable level and that the Force complies with relevant legislation and National ACPO Community Security Policy.

Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is responsible for accepting risk on behalf of the Force. The SIRO in the event of a risk being deemed to high for the Local Accreditor to accept, will make a decision on whether to accept the level or risk or not. The SIRO works closely with the Local Accreditor to ensure that business risk is being properly managed across the Force. The role of the SIRO is currently the responsibility of the ACC Specialist Operations.

Senior System Owner (SSO)

The Senior System Owner is the chief officer of Departmental Head who is responsible for a particular information system. This individual owns the systems Risk Management and Accreditation Document Set (RMADS) and is responsible for authorising users and changes to the system. The SSO is responsible for ensuring that the system complies with Force Information Security Policy (FISP).

The Force Information Security Officer (FISO)

The FISO acts as the Single Point of Contact for Information Security and is responsible for the day to day management of the Information assurance function within SWP. The FISO also fulfils the following roles, as outlined in HMG Security Policy Framework (SPF): Departmental Security Officer (DSO), IT Security Officer (ITSO), Local Accreditor, and Communications Security Officer (ComSO).

Departmental Security Officer (DSO)

As outlined in the HMG Security Policy Framework the DSO is responsible for the day to day management and supervision of information security risks to a government department. All police forces are seen as separate departments and therefore HMG policy dictates that each police force must have a designated DSO. The DSO acts as the Single Point of Contact for Information Security and is responsible for keeping the SIRO up to date on business risks associated with Information. HMG Policy requires that the DSO must have direct access to the SIRO. HMG Security Policy Framework (SPF) recommends that the DSO should have day to day management of the Information Security, Physical Security and Personnel Vetting functions within a government department. The DSO role is currently a part of the Force Information Security Officer (FISO) role.

The IT Security Officer (ITSO)

The ITSO is responsible for ensuring that the relevant security controls are in place for the ICT infrastructure and is also responsible for reviewing and advising on the Security Operating procedures (SyOps) for key internal systems. The ITSO is also responsible for managing the annual IT Health Checks on ICT infrastructure and for advising projects on ICT security risks. In most government organisations the ITSO is subordinate to the DSO, but in SWP, both of these roles are undertaken by the Force Information Security Officer (FISO).

Local Accreditor

The Local Accreditor is responsible for ensuring that the Force complies with HMG Policy on accreditation of information systems. All systems within SWP must be formally accredited if they, process, transmit or store protectively marked information of PROTECT or above. The Local Accreditor reviews the RMADS and makes a risk assessment using HMG Guidelines and decides whether to accept the residual risk. If the Local Accreditor for whatever reason is unable to accept the residual risk, then the issue is escalated directly to the SIRO for a decision. This role is currently carried out by the Force Information Security Officer (FISO).

Communications Security Officer (ComSO)

The ComSO is responsible for ensuring that the Force complies with HMG Policy in regard to Cryptographic material and secure communications as outlined in HMG IA Standard No. 4. The role is currently carried out by the Force Information Security Officer (FISO).

SPECIFIC GUIDANCE – Physical Security

PROCEDURAL HEALTH AND SAFETY CONSIDERATIONS
NONE

SPECIFIC PROCEDURES

Introduction

Physical security involves the appropriate layout and design of facilities, combined with suitable security measures, to prevent unauthorised access and protection of SWP assets, which include people, information, materials and infrastructure. This means putting in place, or building into design, measures that prevent, deter, delay and detect, attempted or actual unauthorised access, acts of damage and/or violence and triggers an appropriate response.

Defence in Depth

SWP understands that effective physical security involves a number of distinct security measures which form part of a 'layered' or 'defence in depth' approach to security, which must take account of the balance between prevention, protection and response. Physical security measures or products as locks and doors are categorised according to the level of protection offered. This is documented in the CESG SEAP Catalogue, available form the FISO.

The 'layered' approach to physical security which SWP have adopted starts with the protection of the asset at source (e.g. creation, access and storage), then proceeds progressively outwards to include the building, estate and perimeter of the establishment. Approach routes, parking areas, adjacent buildings and utilities/services beyond the perimeter should also be considered. To ensure appropriate physical security controls, the Force has considered the following factors:

- The impact of loss of the site or asset;
- The level of threat;
- The vulnerability;
- The value, protective marking or amount of material held;
- The particular circumstances of the establishment, including considerations of environment, location and whether occupancy is sole or shared.

Departments must ensure that before they authorise a computer terminal in a building to access SWP network, that the FISO is involved so that they can do a security audit to determine whether the location and security controls in place are adequate.

Storage of Sensitive Assets

Critical, sensitive or protectively marked assets must be located in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls.

The FISO's use the HMG Physical Assessment Questionnaire and the Physical Security Baseline Controls Matrix to identify the appropriate physical security measures to be put in place, based on the protective marking of the material to be stored.

Secure Containers

For large quantities of protectively marked material, or for particularly sensitive documents, CESG has approved a number of security containers. The FISO has a catalogue of these products and it is strongly recommended that any department using such sensitive material contact the FISO to ensure that they have an appropriate secure container.

Secure Rooms

For particularly large amounts of inherently valuable removable items, a Strong Room must be used. For more information please contact the FISO.

Office Areas and a 'clear desk' policy

SWP have decided that in most areas, a clear desk policy is impractical and have instead adopted a more practical solution which is to lock away any sensitive documents in a cupboard and then lock the room at the end of the night.

Building Security

The Facilities security department along with the FISO routinely perform out of hour's security audits and report their findings to the heads of the respective departments and the ISB.

When a new office building is being planned it is a mandatory requirement for the department or BCU Commander to inform both the Facilities Manager and the FISO, so that they can be involved in the design process. This is to ensure that proper physical security controls are put in place prior to any sensitively marked information assets being stored on the premises.

Physical Access Controls

Police officers and Police Staff are required to display their badges or warrant cards at all times, while on SWP premises.

Physical access control within SWP has been achieved through a combination of manned guarding and mechanical and technical controls. Frontline security staff such as security guards and receptionists play a vital role in controlling access to SWP premises, but to assist them in their duties, SWP have also implemented:

- Automatic Access Control System (AACS), via a swipe card;

- Have issued all staff with ID Badges, which staff are required to wear at all times while on SWP premises;
- Visitor Control – all visitors must be escorted for the entire duration of their visit by a member of the department which the person is visiting. It is the head of departments responsibility to ensure that any visitors to their area are properly supervised at all times;
- In some areas, CCTV is in operation;

Frontline staff are likely to be exposed to a higher level of risk than others. This should be considered in the risk assessment and additional protections and training must be put in place as required.

HMG Security Policy Framework, has the following mandatory requirements for all departments including Police Forces:

- **Mandatory Requirement 56** – Departments and Agencies must control access to their estate using safeguards that will prevent unauthorised access;

- **Mandatory Requirement 57** – Departments and Agencies must have plans and procedures for dealing with and intercepting unauthorised visitors or intruders. Such plans must include the ability to systematically search the establishment if necessary;

- **Mandatory Requirement 58** – Departments and Agencies must ensure that access control policies are made available to all staff and that staff are briefed on their personal responsibilities (e.g. wearing a pass at all times and escorting visitors and searching their work area if required).

Incoming Mail and Deliveries

SWP have procedures in place to deal with deliveries to SWP HQ and are in the process of implementing a system to screen incoming mail deliveries for suspicious items.

Perimeter Security

In response to the below HMG Secure Policy Framework mandatory requirements:

Mandatory Requirement 61 – Department and Agencies must establish a secure perimeter, with appropriate security barriers and entry controls. Perimeters should offer physical protection from unauthorised access, damage and interference and allow for quick identification of suspicious individuals or unusual items.

Mandatory Requirement 62 - Departments and Agencies must first produce a detailed Operational Requirement before deciding to deploy a security measure, particularly when purchasing a system or security product. This should clearly define what the system is expected to achieve.

Mandatory Requirement 63 – The deployment of CCTV must be in accordance with the Data Protection Act 1998.

Categorisation of the Government Estate

SWP is considered a potential target for terrorist attack or hostile interest. The Government establishments are assessed on a three category risk assessment, consisting of HIGH, MODERATE and LOW.

The terrorist threat level to SWP premises is available on the Force Intranet.

Threat Levels

The Government threat levels are designed to give a broad indication of the likelihood of a terrorist attack. The threat levels are LOW, MODERATE, SUBSTANTIAL, SEVERE and CRITICAL. These five levels reflect an assessment of probability of attack based on an analysis of terrorist's intentions, targeting priorities, capabilities and any evidence of current planning and timescales. Information on the SWP threat level is available on the Special Branch Website on the Force Intranet.

Government Estate Response Level System

The Cabinet Office operates a system of response giving Forces a broad indication of the level of protective security readiness required at any one time. The Response Level is informed by the level of threat as well as specific assessments of vulnerability and risk to SWP, but Response Levels tend to relate to sites, whereas Threat Levels usually relate to broad areas of activity. The Three Response Levels are: NORMAL, HEIGHTENED and EXCEPTIONAL.

Precise measures adopted for each individual site and at each Response Level are the responsibility of the Departmental Security Officer (DSO), which is one of the roles filled by the Force Information Security Officer (FISO). The FISO adopts these measures in consultation with CPNI and specialist Counter-Terrorist Security Advisors and these measures must form part of CT planning. Some of these measures deployed include restricting access, increasing patrols and frequency of bag searching, however a more detailed description of incremental security measures is set out in the supplementary material of the HMG Security Policy Framework (SPF).

Counter-Terrorist Protective Security Policy and Plans

SWP have developed security policies in relation to Counter-Terrorism in accordance with advice from national security authorities, these must also be included as part of Business Continuity Plans.

For more information on how Counter-Terrorism please see the WECTU website on the Force Intranet.

INDIVIDUAL ROLES AND RESPONSIBILITIES

The Facilities Manager

The Facilities Manager is responsible for overseeing the physical security of the various SWP sites. The Facilities Manager works closely with the Force Information Security Officer to ensure that the physical security is compliant with Force Policy. Along with the FISO, the Facilities Manager routinely performs night security audits on SWP HQ.

Gatehouse Security Officers

The Gatehouse Security Officers are responsible for ensuring that the HQ site is properly secured and they have a number of responsibilities relating to physical security, including security walks.

Force Information Security Officer (FISO)

The FISO is responsible for the day to day management of Information Security and works closely with the Facilities department to ensure that the physical security controls are compliant with Force Policy. Along with the Facilities Manager, the FISO routinely performs night security audits on SWP HQ.

Police Officers and Police Staff

All members of SWP are responsible for ensuring that there areas are secure and that any individuals failing to identify themselves. All members of SWP must either identify themselves while at HQ by displaying their warrant cards or badges. All members of SWP must report any physical security breaches to the Gatehouse Security Officers, the Facilities Manager or the FISO.

SOUTH WALES POLICE
FORCE POLICIES & PROCEDURES

SPECIFIC GUIDANCE – Business Continuity Management

PROCEDURAL HEALTH AND SAFETY CONSIDERATIONS
NONE

SPECIFIC PROCEDURES

What is Business Continuity Management

The British Standard on Business Continuity Management (BCM), BS 25999 defines BCM as a "holistic management process that identifies potential threats to an organisation and the impact to business operations of those threats, if realised might cause and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation and value creating activities."

Business Continuity Management (BCM) is the process through which BCU's and Departments aim to continue their critical business activities following a disruption and effective recovery afterwards (return to normal). It is an essential aspect of securing our business.

Mandatory Requirement 70: Departments and Agencies must have robust, up to date, fit for purpose and flexible business continuity management arrangements that are regularly tested and reviewed and supported by competent staff that allow them to maintain, or as soon as possible resume provision of key products and services in the event of disruption.

An effective BCM programme will have the following features:

- A BCM strategy endorsed and supported by Board level management;
- A BCM programme appropriate to the size and complexity of the department;
- Planning to proportionately manage the impact of events and recover from them;
- BCM arrangements that are exercised, reviewed and renewed as appropriate for the organisation and supported by adequately trained staff;
- Communications that ensure that all staff are aware of the BCM arrangements and of their responsibilities within them;

The outcomes of an effective BCM programme are that:

- Key assets are protected and services are identified and protected, ensuring their continuity;
- An incident management capability is developed to provide an effective response;
- The organisations understanding of itself and its relationships with other

departments and organisations to include Local Authorities and other emergency services is properly developed, documented and understood;
- Staff are trained to respond effectively to an incident or disruption;
- Stakeholder requirements are understood and able to be met;
- Staff and stakeholders receive adequate support and communications in the event of a disruption;
- The organisations supply chain is secured;
- The organisations reputation is protected;

As a police force it is essential that in the event of a disruption such as loss of electrical power or a flood, SWP are still able to provide the key business services to the public and that normal business will be resumed in a relatively short period of time. To this end it is the responsibility of every BCU Commander and Department Head to ensure that their area of responsibility has adequate Business Continuity plans available to ensure compliance with this policy and that these plans are tested at least annually.

INDIVIDUAL ROLES AND RESPONSIBILITIES

BCU Commanders and Department Heads

Are responsible for ensuring that their departments have Business Continuity Plans in place to ensure that in the case of an incident the department can still give an acceptable level of service, to the public and other departments within the Force.

Line Managers

Are responsible for ensuring that their individual units have plans in place to be able to continue their function in case of a disaster.

Users

Are responsible for ensuring that they comply fully with any Business Continuity Management (BCM) plans which maybe in place.

Civil Contingencies and Resilience Unit

Is responsible for managing the Forces commitment to the Civil Contingencies Act and to ensure that the Force has robust BCM procedures in place.

SPECIFIC GUIDANCE – E-Mail and Internet Use

PROCEDURAL HEALTH AND SAFETY CONSIDERATIONS
None

SPECIFIC PROCEDURES

Introduction

South Wales Police provides access to a wide range of resources, including those available from the Internet, in supporting both operational frontline officers and police staff.

The following section outlines, the acceptable use of these resources including but not limited to Internet Access, E-Mail, FIS and other resources that are used day to day by staff to effectively carry out their roles.

Purposes of Use

The Internet, Intranet (FIS) and e-mail are to be used for **policing purposes only**, in accordance with PACE and other relevant legislation. A 'policing purpose' includes **any duties that SWP employees are required to undertake as part of their day-to-day policing work.**

Acceptable Use

Some **acceptable** uses of the Internet/E-mail facilities would include:

- Legitimate SWP business.
- Approved Trade Union or staff association activities.
- Viewing, displaying or downloading information or images that would otherwise contravene the Acceptable Use of Internet Facilities as described in this policy, providing it is in the course of the person's duties and approval has been formally authorised by the manager and FISO informed.
- Accessing legitimate chat rooms or on-line forums related to SWP or Police business, such as a criminal investigation.

Prohibited Use

Internet, Intranet (FIS) and e-mail facilities are **NOT** provided for personal use, and in particular must not be used by any SWP employee without proper authorisation to:

- Accessing or sending pornographic material or material that may be considered to be offensive;
- Carry out research in connection with private study;
- Conduct personal, private or freelance business interests;
- Conduct political activities;
- Download or play interactive games;
- Engage in gambling;
- Participating in or accessing personal chat sessions in Chat Rooms;
- Post abusive or insulting messages or ones that criticise other individuals or organisations;
- Post information that harasses, abuses, threatens or bullies others;
- Post personal or sensitive information about an individual;
- Take part in or create electronic chain letters;
- Accessing personal E-mail accounts [e.g. Hotmail, Yahoo mail]
- Downloading music, screen savers or any other media that is not related to Police business.
- Downloading Freeware or Shareware software – unless specifically authorised by the Assistant Director – Corporate Information and Technology;
- Downloading or copying material that is protected by copyright legislation
- Political activity [excluding approved Trade Union, Police Association or staff association]
- Personal on-line shopping.
- Streaming data to desktops [e.g. News tickers, share prices etc.]
- Publishing any protectively marked [GPMS] '**RESTRICTED'**, or above. [Only information that is **'NOT PROTECTIVELY MARKED'** can be published, providing it is suitable for public viewing.]
- Forwarding protectively marked information above NOT PROTECTIVELY MARKED to a non secure e-mail address (non secure means an address other then .pnn, .gsi, .gsx, .cjsm)

Note: In 2000 changes in The Data Protection Act made "Browsing" of police systems for reasons other then business related use, a criminal act and makes the individual liable for prosecution. This includes systems that because of your role, you have administrative access to. For example system administrators may have access to folders to set access permissions, this is a legitimate use, but reading or browsing the information in those folders would be considered a criminal offence under the Data Protection Act.

Browsing or 'surfing' the Internet for information should only be undertaken in connection with work related reasons.

Monitoring of Use

All Internet and e-mail usage is monitored by the Information Management Unit.

Requesting external E-mail

Standard access to e-mail is given when the user is first given their domain account. If for any reason a user needs access above what a standard user needs then they must fill out the CJX Internet/E-mail access form <Insert Link> this form needs to be approved by your line manager and then e-mailed to CJXAUTH.

The process for changing someone's access rights to e-mail can take several days.

Gaining access to the Internet

Access to the internet is given as part of a users domain account access, this access is restricted to standard sites which is all most users will need.

It is understood that some users may require access to the Internet above what a normal everyday user would need. The process for gaining a higher level of access for the Internet is the same as that for gaining higher access to E-mail, mentioned above.

Downloading Software

Downloading any software [including fixes and patches] should be performed only by staff authorised to do so by the Assistant Director – Corporate Information and Technology. Appropriate licensing or agreements must be in place. All downloaded software must be checked for viruses.

Business transactions

Any business transactions made using the Internet will be with trusted organisations or approved partners, and only for Police related business. All transactions will be in line with the current purchasing policies and procedures. The Internet should not be used to by-pass these controls.

Data Protection

Any personal information published on the Internet must be permitted under the organisation's notification under the Data Protection Act 1998.

Group Mailboxes

A group mailbox can be established for a department or unit, but the head of the department takes ownership of the group mailbox and accepts responsibility for the use of it. All group mail boxes must be authorised by the head of department or a properly authorised delegate.

Force Information Broadcasts

All Force Information Broadcasts must be authorised by the BCU Commander/Head of Department or a suitably authorised deputy. Force Information broadcasts must be sent to the Information Management Unit and should include the name of a contact within the department requesting a broadcast.

The broadcasts will then be graded (Gold, Silver or Bronze) and then sent to SWPHELPDESK for it to be broadcast.

Departments are responsible for formatting and creating the broadcasts and ensuring their accuracy. The Information Management Unit cannot be responsible for the wording or accuracy of Force Broadcasts.

Force Information Broadcasts must only be sent out following the procedure outlined above. Officers or staff must not send out their own broadcasts, this includes sending out an e-mail in batches (for example 50) to get around the system as this would be in breach of this policy and could lead to disciplinary action.

Forwarding E-mails from your SWP address

Users are reminded that they must **not** forward any e-mails of a protective marking above NOT PROTECTIVELY MARKED from their work accounts to a non secure address. (The only secure addresses are .pnn, .gsi, .gsx, .mod, .cjsm, ***any other*** addresses are not secure).

INDIVIDUAL ROLES AND RESPONSIBILITIES

BCU Commanders

Are responsible for ensuring that any Force Broadcasts issuing out of their BCU's are appropriate and accurate and comply with this policy.

Force Information Management Unit

Is responsible for ensuring that the broadcast includes contact details of the requesting department or BCU and assigning them a grading (Gold, Silver or Bronze). The Force Information Management Unit is responsible for sending the broadcasts to the ICT Service Desk.

Users

It is everyone's responsibility to comply fully with the guidance given above, any employee fails to comply with the above guidance, could be disciplined. This could include a suspension of service (Internet or E-mail) or formal discipline such as verbal or written warnings.

The SWP Information Management Unit and Professional Standards Department have the ability to monitor all internet access and e-mail traffic in order to enforce and report on adherence to the above guidance.

SOUTH WALES POLICE
FORCE POLICIES & PROCEDURES

SPECIFIC GUIDANCE – *Mobile Computing*

PROCEDURAL HEALTH AND SAFETY CONSIDERATIONS
NONE

SPECIFIC PROCEDURES

What is Mobile Computing

Mobile Computing is using various ICT related devices to access information outside the SWP office environment. Mobile computing includes using laptops, PDA's such as Blackberry's and USB Storage pens to work on SWP information. This poses a number of threats to that information, which this policy aims to address.

Threats Inherent to Mobile Computing

There are a number of threats which are unique to mobile computing, these include:

- Losing mobile computing devices;
- Being overlooked or overheard, which is called shoulder-surfing or eavesdropping;
- How the mobile computer device accesses internal SWP systems;
- Someone gaining access to the information on a lost or stolen mobile device;
- Disposal and decommissioning of mobile computer devices;

All the devices listed below are provided for business use only, users are not to use these devices for any other use unless specifically authorised by their BCU Commander, Department Head or FISO to do so.

Laptops

A number of laptops have been provided by departments for staff to work from home occasionally or to facilitate mobile working. These laptops as provided by SWP ICT are appropriately encrypted to CESG standards and therefore comply with HMG Guidance and the Hannigan Data Handling report.

No other laptops other than those supplied by ICT are suitable to hold SWP information unless specifically approved by FISO and the Assistant Director Corporate Information & Technology.

Any lost or stolen laptops must be reported to FISO at the earliest opportunity. The users is responsible for ensuring that if the laptop is being used in a public place, then the information being displayed cannot be compromised by people close by.

SWP issue laptops must be kept with the user at all times or in a secure location when not in use, for example in a secure hotel safe. No unauthorised person should be given access to the laptop unless prior permission has been sought from the Department Head and FISO.

PDA's and Blackberry's

SWP are currently in the process of issuing all front line police officers with a Blackberry to allow mobile access to key SWP systems. Each of these Blackberry's are to be considered SWP issue and are not for private non business use unless explicitly approved by the Department Head or BCU Commander.

Any lost or stolen PDA's must be reported to FISO at the earliest opportunity. Use of the PDA is strictly restricted to authorised users only. SWP issue PDA's as provided by the Mobile Working project to Police Officers are suitable for handling and transmitting RESTRICTED information, therefore these PDA's can be used for normal police business. These PDA's are not currently suitable for CONFIDENTIAL systems such as ViSOR, HOLMES and PND, no CONFIDENTIAL information is to be stored or transmitted via a SWP issue PDA, as issued to police officers via the Mobile Working project.

USB Removable Mass Storage devices

SWP currently issue to staff encrypted Kingston USB Mass Storage devices to allow for mobile working. These devices are encrypted up to AES 256, but are currently not approved by CESG for storing RESTRICTED information. A risk managed decision has been made by the Information Security Board (ISB) to allow these devices to be used for RESTRICTED information. Only SWP or other police information is to be held on these devices and they are reserved for business use only.

These devices are not currently appropriate for CONFIDENTIAL information and therefore no information marked CONFIDENTIAL should be stored on these devices unless it is operationally urgent and has been improved by the BCU Commander or Department Head and FISO.

Lost or stolen USB Mass Storage devices must be reported to FISO at the earliest opportunity.

Disposal of Mobile Working devices

All mobile devices which are ready for disposal must be disposed of in accordance with their respective protective marking. In regard to mobile devices the protective marking is RESTRICTED.

Therefore any devices to be destroyed or de-commissioned must be returned to ICT for secure disposal. No user is to take it on themselves to dispose of the mobile device as the device may still hold sensitive information which could be compromised. Any user, who disposes of these devices not in line with the policy above, is in breach of the policy and could be disciplined by Professional Standards.

Threats inherent to Mobile Computing
When using mobile computing facilities, e.g. notebooks, palmtops, laptops and mobile phones, special care must be taken to ensure that business information is not compromised.

Care must be taken when using mobile computing facilities in public places, meeting rooms and other unprotected areas outside of the organisations premises. Protection must be in place to avoid the unauthorised access to or disclosure of the information stored and processed by these facilities, e.g. by using cryptographic techniques.

It is important that when such facilities are used in public places care is taken to avoid the risk of overlooking by unauthorised persons. Procedures against malicious software must be in place and be kept up to date. Equipment must be available to enable the quick and easy back-up of information. These back-ups must be given adequate protection against, e.g. theft or loss of information.

Suitable protection must be given to the use of mobile facilities connected to networks. Remote access to business information across public network using mobile computing facilities must only take place after successful identification and authentication and with suitable access control mechanisms in place.

Mobile computing facilities must also be physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centres and meeting places. Equipment carrying important, sensitive and/or critical business information must not be left unattended and where possible, must be physically locked away, or special locks must be used to secure the equipment.

Training must be arranged for staff using mobile computing to raise their awareness on the additional risks resulting from this way of working and the controls that must be implemented.

INDIVIDUAL ROLES AND RESPONSIBILITIES

BCU Commanders and Department Heads
Are responsible to ensure that any users within their section who need Remote Access are identified and properly managed.

ICT Department
The ICT department are responsible for ensuring that the way remote users connect to Force systems is secure and well managed in line with this policy.

Line Managers
Are responsible for ensuring that any members of their team who are accessing SWP information remotely are familiar with this policy and are complying with it.

Users
Are responsible for ensuring that they are familiar with this policy and are compliant with it.

SOUTH WALES POLICE
FORCE POLICIES & PROCEDURES

SPECIFIC GUIDANCE – *Mobile Phone Technology*

PROCEDURAL HEALTH AND SAFETY CONSIDERATIONS
NONE

SPECIFIC PROCEDURES

The Use of Mobile Phones within SWP

Communications are vitally important for SWP in the day to day business activities, for this purpose, SWP have issued mobile phones to certain individuals.

Mobile phones enable SWP officers and staff to be able to communicate more or less anywhere and therefore provide a significant advantage to the Force.

However, mobile phone technology also poses a number of threats to the Force if the technology is not used correctly or securely. This policy addresses the acceptable use of mobile phone technology and is mandatory for all SWP employees.

This policy covers the following areas:

- Procuring mobile phones for the Force;
- Issuing mobile phone to SWP employees;
- Acceptable use of SWP issue mobile phones;
- Reporting lost or stolen SWP issue mobile phones;
- Use of non-issue (personally owned) mobile phones for police business;
- Disposal of mobile phones;

Procuring Mobile Phone Technology for the Force

It is recognised that for the Force to function efficiently, it has become necessary for certain individuals to be provided Force issue mobile phones.

With the roll out of Blackberry's to all front line Police Officers, by definition as voice is enabled on these devices all front line Police Officers now have Force issue mobile phone devices.

When procuring mobile phone technologies, the department responsible should take care to ensure where possible that the phones only include technology which is expressly needed by the Force. For example currently the only technology needed is voice and text functionality. Therefore any phones procured for the Force should only have this technology available, any other technology such as Bluetooth, MP3 devices should be disabled by default or not included on the device in the first place.

The procuring department should ensure that when purchasing mobile phones,

they only purchase mobile phones with the bare minimum of functionality needed by the Force.

Any such purchases should be vetted by the FISO for approval prior to being bought.

The following guidelines are recommended for Force mobile phone procurement:

- Mobile phones should not include Bluetooth capability, if this is not possible then Bluetooth must be disabled, unless authorised by the Head of Department and approved by FISO;
- Mobile Phones should not include cameras where possible, if they are included then they should be disabled as standard;
- Mobile phones should not include MP3 players if possible, or they should be disabled as standard;
- Mobile phones should only have large enough storage capacity to allow for normal address, phone book activities. For example phones with large (several gigabytes) of storage capacity are not recommended;
- WAP (Web and mail) access should not be included on Force issue mobile phones or should be disabled as standard;

By following these guidelines the risk of mobile phone technology to the Force is mitigated.

Issuing mobile phones to Force employees

Before issuing mobile phones to employees, departments must have a process in place to enable the user to sign a declaration that says that they will comply with this policy in relation to their use of Force issue mobile phones and that they have read the Mobile Phone usage guidance outlined in the Information Security Handbook. The signed form must be kept by the department issuing the mobile phone, for the life of that particular phone.

Once this is done the user may be issued a mobile phone.

Acceptable use of SWP issue mobile phones

The following comprises an acceptable use policy for Force issue mobile phones:

- Force issue mobile phones must only be used for business purposes, any other usage is strictly prohibited unless authorised by the users line management;
- Care must be taken when using Force issue mobile phones as they are only approved for NOT PROTECTIVELY MARKED information;
- In case of an emergency (operational criticality) the user may talk at RESTRICTED, but must use guarded speech;
- The user must report any lost or stolen Force issue mobile phones to their line management and FISO at the earliest available opportunity;
- The user must not:
    - Access or send material which may be considered to be offensive;
    - Conduct personal, private or freelance business interests;
    - Conduct political activities;
    - Send or transmit abusive or insulting messages or ones that

criticise other individuals or organisations;
- Send or transmit information that harasses, abuses, threatens or bullies others;
- Political activity [excluding approved Trade Union, Police Association or staff association]

- The user must not dispose of Force issue mobile phones themselves, but bring them back and hand them into the issuing department;

Any breach of the above policy may result in disciplinary action being taken by Professional Standards.

Reporting lost or stolen SWP issue mobile phones

It is the user's responsibility to ensure that they report lost or stolen mobile phones at the earliest available opportunity to their line manager and FISO.

The report can be issued via telephone or via the incident reporting tool on Force Intranet, found under tools. Or the user can report the lost or stolen phone to the FISO via e-mail.

Use of non-issue (personally owned) mobile phones for police business

Only Force issue mobile phones should be used for SWP business, however occasions may arise when it is necessary to use a personal mobile phone for SWP business, such as in an emergency.

If it becomes necessary to use a personal mobile phone for SWP business then the acceptable use policy outlined above, still applies, for that phone call.

Disposal of mobile phones

Force issue mobile phones, must be disposed of securely when they reach end of life or are being replaced by new ones. The old phones must be brought back to the Force and handed into their line manager (who must keep note of this along with the issuing note) so that they can be securely destroyed.

Users are not to dispose of the mobile phone themselves as this is against this policy and could result in disciplinary action being taken.

Use of Mobile Phones in Secure Areas

For operational and security reasons, there is a restriction on the use of mobile phones in certain areas of the Force. These may include areas such as Public Service Centre, Public Protection, Hi-Tec Crime, and Major Crime. It is up to Head of Department to determine whether to ban the use of mobile phones in such secure areas.

INDIVIDUAL ROLES AND RESPONSIBILITIES

Finance and Business Services Directorate

This department is responsible for ensuring that any mobile phone technology procured for the Force, comply with this policy and that during this process the Force Information Security Officer(S) is consulted.

BCU Commanders and Department Heads

These are responsible for ensuring that any mobile phones procured for their department or BCU is procured through the SWP contract and that there procurement complies with this policy.

Line Managers

Are responsible for ensuring that anyone within their team who possesses a mobile phone issued by SWP, are familiar with and are complying with this policy.

Users

Are responsible for ensuring that they comply with this policy and only use Force Issue mobile phones/PDA's for business purposes.

Personal mobile phones should only ever be used for Force business as a matter of operational necessity or emergency.

SOUTH WALES POLICE
FORCE POLICIES & PROCEDURES

SPECIFIC GUIDANCE – *Remote Working*

PROCEDURAL HEALTH AND SAFETY CONSIDERATIONS
NONE

SPECIFIC PROCEDURES

Remote Working (working on official information away from official premises)

The guidance in this section is intended to cover the main security issues relating to the physical, document, IT communication systems security controls applicable when working on official information away from official premises, that is, remote working. Where individuals are required to work on official information overseas specific security guidance will be needed because of the differing levels of threat posed by the country or countries involved.

Remote working embraces both mobile working and Teleworking, as defined in ISO 27001:2005 as outlined above. It refers to work in a place away from the official premises of the sponsoring department, agency or contractor. The guidance in this section covers homeworking and other types of remote working, for example, in hotel rooms, at conference venues. It is assumed that remote working is inherently less secure than when working in a controlled environment of official premises where levels of security in place is determined by the level of threat to that organisations and its assets.

SWP currently does not allow homeworking.

Direct access to host systems by the remote user is called remote access. In some cases remote workers access their host system from another network (for example when embedded in a partner agency or customer organisation), making use of a network-level connection between the partner or customer IT system and their own organisations IT system.

Authorising Remote Working

Remote working on official information, whether at home, in hotels or other places away from official premises, must only be authorised when it has been assessed that the risks can be effectively managed. Authority to work remotely on official information and responsibility for deciding on appropriate security controls must rest with the BCU Commander or Head of Department in consultation with FISO.

Departments must ensure that when individuals are authorised to work remotely on official information that they are aware of the appropriate physical, document and IT security controls needed to provide required levels of protection before the work begins.

Resources Needed by the Remote Worker

The technologies needed by a remote worker are likely to vary depending on the nature of the tasks involved and on the level of interaction with colleagues located elsewhere. In most cases SWP provide the user with a laptop.

Assessing the Risks

When individuals work remotely on official information in the absence of appropriate security controls, including procedural controls and other less formal safeguards, such as the presence of colleagues, there is an increased risk of deliberate or accidental compromise.

In the UK, the threat associated with remote working may be lower than at official premises, where there may be an implied association with sensitive information. This may not apply where an individual's work (for example overseas service or contact with foreign missions) may have led to them being identified as having access to sensitive information. However, the vulnerabilities associated with remote working are likely to be greater than at official premises. Similar reasoning applies when determining the threat to individuals from terrorist and single-issue groups who are capable of identifying the homes of potentially vulnerable individuals.

A remote worker also faces threats that are not necessary directly linked to their employment. These include equipment and accidental or deliberate overlooking or eavesdropping. Continuous personal custody is rarely realistic and in some circumstances may be insufficient. For example IT equipment is highly attractive to thieves and muggers. IT threats are likely to be higher for the remote worker and could include:

- **Theft;**
- **Viruses;**
- **Hacking;**
- **Abuse of access rights;**
- **Interception – local and remote eavesdropping;**
- **Incorrect operation of transmission equipment;**
- **Denial of service;**

It is rarely realistic to expect to achieve in the home or other remote working places the level of security that pertains in official premises. The vulnerabilities connected with remote working include:

a. Weak physical defences;
b. Poor IT discipline, for example, the use of insecure hardware and software, the use of unapproved network connections, introduction of malicious software to the remote worker and sponsoring department or agency systems;
c. Insecure handling of documentation and electronic communications;

Special consideration must be given to the configuration of equipment used for remote access to departmental or agency systems.

Managing the Risks

Whether the remote working involves the use of IT or simply the reading of documents, personnel acceptance of responsibility for the protection of the assets involved is fundamental to good security practice.

The security procedures required for remote working are likely to include both technical and non-technical controls. Such controls will depend in a residual risk assessment taking account of the levels of protective marking, if any (confidentiality), the requirements for business continuity (availability) and for preserving the integrity of information. This assessment must be undertaken by the FISO, prior to authorisation being given. In addition to specific controls consideration must be given to:

a. How assets are to be registered and accounted for;
b. If a monitoring regime is to be put in place;
c. If the written agreement of the "remote worker" will be required to allow access to their home for audit purposes.

Before official information is handled remotely, departments and agencies must be satisfied that:

a. Remote workers understand and accept their obligations in respect of the security controls necessary for the appropriate protection of the assets involved;
b. All the necessary practical security controls and arrangements are in place;
c. Where applicable, remote workers have been briefed on all security aspects of using IT equipment installed in the remote location;
d. Where networking is required, the total system, often referred to as the domain, has been "accredited";

Accreditation is the formal assessment of an information system against its information assurance requirements, resulting in the acceptance of residual risk in the context of business requirement. It is a prerequisite to approval to operate.

Physical Security

Mobile Remote Working within the UK

Theft loss, overlooking and eavesdropping are the greatest risks when an individual is required to work remotely on official information while travelling. Mobile employees will often be at locations offering even lower levels of privacy then at home and it is essential that a high level of vigilance is maintained.

Normally, protectively marked assets must remain in the individual's personal control and must not be set down in a public place. They must not, for example, be left in a cloakroom, or left unattended on a train while the individual is away from their seat. When it is necessary to work remotely on official information, storing that information electronically, protected by an appropriate data-at-rest encryption product, can provide better security – in terms of confidentiality – then storing the same data in paper form.

Mobile Remote Working (outside the UK)

UK-Based Employees

The threat to the remote worker overseas is generally greater than in the UK. In addition to the greater threat from deliberate theft of sensitive information, there may also be a greater threat from eavesdropping and interception. Individuals must take guidance from their FISO on the local threats. Appropriately protected laptops may be usable but there may be handling constraints on the use of cryptographic material in some countries. Users must be aware of the legal issues regarding the use of cryptography in some countries, for example France.

Overseas-based Employees

The situation needs to be assessed by the FISO on a country-by-country basis. The threat may be significant where intelligence services have longer to plan and conduct covert operations. Even in notionally friendly countries it is not advisable to work outside of secure premises without a full prior assessment of the risks.

IT Security

The following areas of IT Security must be considered before authorising remote working on protectively marked assets:

- **Equipment;**
- **Access Control;**
- **Data Storage;**
- **Virus Control;**
- **On-Line Working and E-mail connectivity;**
- **Authentication;**
- **Internet Access;**

Equipment

Remote IT equipment, even when off-line, must be regarded as an extension of the workplace system. It requires the same effective levels of physical, technical and procedural security. Remote working must be carried out using dedicated IT equipment, with all the hardware and software supplied and controlled by the sponsoring department within SWP. The use of personally owned IT equipment is not permissible.

Departments must carry out residual risk assessment in consultation with the FISO on the IT systems designated for remote working. This must used on the basis of the risk management decision to accredit the remote system.

Access Control

The residual risk assessment will determine the need for access control mechanisms to protect against unauthorised access. An appropriate identification and authentication system complying with CESG Memorandum No 24, complemented by good physical and procedural security, is fundamental to protecting against unauthorised access. In addition, CESG encryption of data at

rest is required to safeguard the data on the hard disk in the event of loss or theft of the IT equipment. For more information on what is contained in CESG Memorandum No 24, please contact FISO on 20954 or 20-682.

Data Storage

The "deletion" of computer files and data, even after they have been removed from the systems "recycle bin" or equivalent, does no more than make the relevant storage area available for overwriting. Until the storage area is in fact overwritten, the "deleted" information can usually be recovered, with minimal expertise using the Commercial Off The Shelf (COTS) utility software. For this reason the storage device must be securely erased in accordance with HMG Infosec Standard No 5. Remote workers must also be made aware that, even though they may opt to save their work to a floppy disk or other form of external storage device, computer operating system may nevertheless store a copy of this data on the hard drive as part of their normal method of operation. The storage device must therefore be secured according to the highest protective marking of data that has been processed on the IT equipment.

Remote workers, in common with all other computer users, must ensure they take regular data backups that must also be appropriately protected depending on the protective marking of the information.

Physically Securing the Hard Disk

The hard disk requires the same level of physical security as documents of the same protective marking. It is difficult to provide adequate physical security for IT equipment used for remote working. Removable hard disks may be easier to secure physically, but data-at-rest encryption will normally be preferred.

Technically Securing the Hard Disk

The use of CESG approved disk encryption product will reduce the protective marking of data stored on a hard disk. Such encryption may protect the confidentiality of the data, but physical security controls and procedures will still be needed to protect against theft or loss to ensure the continuing availability of the system. Use of data-at-rest encryption brings with it requirements for procedures to ensure the security of encryption keys, passwords and tokens.

Virus Control

Any medium that can be used for storing or transmitting software and data is potentially a virus carrier. Carriers include floppy disks, hard disks, magnetic tape, optical disks, CD-ROMs, e-mail, Internet chat rooms, surfing the web and other network connections. To reduce the risk of a virus infecting systems, remote workers must aim to implement, as a minimum, the following procedures:

a. Where possible, only software, including regularly updated anti-virus software, provided by the ICT department must be used on remote working systems;
b. Connection to networks must be approved in accordance with this security policy;

Dealing With Viruses

If a remote workers computer become infected with a virus the following action must be taken:

a. Immediately disconnect from any on-line departmental system;
b. Implement a virus cleansing and data recovery plan;
c. Immediately report all details of the infection to the Force Information Security Office (FISO) by telephone, not e-mail;
d. Remove the virus and have the PC checked and passed as "clean" by SWP ICT before any attempt is made to reconnect to SWP networks and systems;

Communications Security

Remote workers who are required to transmit information protectively marked CONFIDENTIAL and above must only use secure communications equipment approved by CESG for HMG use. In all cases a risk assessment must be carried out on the basis of the threats associated with remote working and the location in question. In additions to the risk to protectively marked information, cryptographic systems will also incur protective marking and/or handling descriptors. Use of HMG cryptographic systems in such circumstances must receive prior accreditation.

When using cryptographic equipment for remote working, it is essential that users are briefed on the particular vulnerabilities applicable to the proposed environment and are provided with clear security operating procedures. These must be based on the system specific operating instructions, the relevant CESG security procedures for the product and the risk assessment. Please contact the FISO for further details on HMG policy and procedures for communications security and cryptography in remote working environments, and other permanent buildings, mobile platforms and transportable facilities and working with portable systems.

Document Administration

Registration and Filing of Documents and other Assets

Departments will need to make arrangements for the registration of protectively marked assets. Remote workers must keep a single register, bearing an appropriate protective marking, in which to record all documents and other assets that they receive or originate, such as magnetic tapes or sets of slides, marked CONFIDENTIAL or above.

Assets originated and passed by the department must be recorded in the register by the worker, with details of destination and data sent. This entry must be as comprehensive as possible and must include, for example, the file reference where a document is filed, details of all addressee of any asset despatched and the destruction of documents or other assets.

Photocopying and Printing

Remote workers must be reminded of the importance of limiting, as far as possible, the copying and printing of protectively marked documents. In particular, they must:

a. Observe any limitations on copying implicit in any protective marking, caveat or other special handling instruction included in the text of a document;
b. Resist the temptation to keep working copies of documents for personal reference at a remote work place;
c. Be required to ensure that copies of CONFIDENTIAL and SECRET documents are taken only on departmental premises;
d. Be advised that copies of other documents may be taken on local government copiers provided the copying of RESTRICTED material is carried out by the homeworker – care must be taken to ensure that documents are not read, or identified as official material, by others;
e. Be especially careful when using photocopiers which retain an image of documents copied – repairs and maintenance of such copiers must be carried out by the department or agency;

Remote workers who do not have access in their home to an approved photocopier must ensure that copies of material protectively marked above PROTECT are only made on the SWP premises.

Transmission of Documents and other Assets

The carriage of protectively marked assets to, from and between official premises and remote work places must be conducted in accordance with guidance given elsewhere in this document.

Destruction of Protectively Marked Waste

Protectively marked waste CONFIDENTIAL and above must be returned to the department or agency for secure destruction in accordance with the guidance discussed elsewhere in this document. Departments will need to make arrangements with remote workers for the destruction of waste protectively marked RESTRICTED and above. Even documents with no protective marking may cause embarrassment if disclosed, for example, details of personal records. Non-paper assets may pose additional problems. The remote worker must be advised to ensure that:

a. All paper waste, protectively marked RESTRICTED and below destroyed locally must be shredded or otherwise torn in small pieces before being mixed with domestic rubbish ensuring that protective markings, descriptors and any special handling markings are obscured;

b. Large quantities of paper and other types of protectively marked assets and magnetic and optical media are returned to SWP for destruction – where magnetic media is required for reuse the data must be erased in accordance with guidance discussed elsewhere in

this document.

Maintaining Security

The rapid advance of technology and security products and services will bring with them new methods of communication for remote workers. But these new technologies will also bring new vulnerabilities. It is therefore important that departments provide an effective and on-going programme of education and training for remote workers. All employees who work away from official premises must report all security incidents to FISO. But in the case of a successful electronic attack (whether a directed attack or a virus or worm) those incidents must also be reported in real time to GovCertUK via the FISO. Similarly all communications or cryptographic incidents must be reported via FISO to the governments Communications and Cryptography Incident Notification Reporting and Alerting Scheme (CINRAS).

Remote Access to IT Systems

Remote access occurs when a legitimate user of an IT system accesses that system, electronically, from somewhere other then the normal working premises of their organisation. Remote workers will often have a requirement for remote access to SWP IT systems.

In addition to the general protective measures required for all remote working environments, as described in the sections above, it may be necessary to implement additional protective measures when remote access is required. This is because compromise of the client equipment, in addition to compromising the data held on that equipment, could also potentially compromise the central IT system that the equipment connects to.

General Requirements – Risk Assessment and Accreditation

The Force Information Security Office (FISO) must conduct a Residual Risk Assessment in accordance with HMG Infosec Standard No 1 to select appropriate and commensurate protective measures as part of a remote access solution.

If the system to which remote access is being proposed has onward connections to other systems, including any CJX systems, it is the responsibility of the Accreditor to ensure that the remote access solution does not affect the accreditation of these network level connections.

If the proposed solution will involve remote access from clients geographically located outside the UK, it is the responsibility of the Accreditor to conduct or commission an appropriate threat assessment for the country or countries involved. There may also be legal implications arising from the carriage and use of cryptographic equipment overseas: Accreditor's in this situation must contact the Security Authorities for advice.

General Requirements – Protecting the Network

Regardless of the protective marking of the network or client, the following requirements must be met:

- **The server must allow connections only from approved and suitably authenticated clients;**
- **The server must record all remote connection activity, including both successful and unsuccessful connection requests;**
- **A protective monitoring policy must be established, appropriate to the impact level of the system being protected;**

General Requirements – Protecting the Client

Regardless of the protective marking of the network or client, the following requirements must be met:

- **Only SWP owned client devices must be used. This is because of the difficulty of enforcing adequate technical and procedural security controls on personally owned client devices and the consequent increased risk of electronic attack to the host server(s) when such devices are used instead of officially owned client devices. Exception: if a CESG evaluated auto-boot thin client solution is used, this requirement can be waived for Restricted and NPM systems.**
- **If internet browser software is made available on the client, it must be configured in accordance with current CESG recommendations;**
- **Only software approved for the system must be installed. Users must not download or install unapproved software applications or utilities and technical measures to enforce this policy will be taken whenever practical;**
- **Commercial anti-virus software must be installed on the client, with the virus database on the client updated on a regular basis. It must not be possible for the user to disable or change the settings of the anti-virus software;**
- **The operating system on the client must be kept fully patched (i.e. critical security patches released by the vendor must be installed on the client as soon as possible after they are released). This requirement applies equally to evaluated and unevaluated software products.**

In addition to the above, it is desirable that all removable media devices (e.g. floppy disks, CD and DVD drives, USB memory sticks) must be disabled for all users (other than, if necessary, system administrators). So that data can only pass from and to the client via the official remote access connection. Allowing the use of removable media devices significantly increases the risk of potentially sensitive material form the host system being transferred without authority to other systems. During the risk assessment process, the Risk Assessor must implement this countermeasure unless an overriding business requirement for access to such devices exists, in which case the Risk Assessor must document this and put in place all reasonable technical and procedural measures necessary to mitigate the risk to an acceptable level.

Specific Requirements for Remote Access to RESTRICTED Systems

A client which connects to a RESTRICTED network must be protected by

BASELINE grade whole disk encryption when turned off/powered down.

When logging into the client device, user authentication must be carried out in accordance with CESG Inforsec Memo 24 (contact FISO for details) and its subsidiary documents.

If connecting via a public IP-based network, protective measures must also be put into place to guard against network attack. The measures required depend on the method used to ensure the confidentiality of the data in transit:

- **If a BASELINE link or network encryption device is used, then a separate evaluated firewall must be installed at the server end of the connection (placed between the Enhanced Grade Encryption device and the Internet connection). The EAL level of the firewall must be determined after an IS1 risk assessment for the system in question. No additional boundary control protection is necessary at the client end unless this is specified in the handling instructions for the cryptographic device (in which case the EAL level of the client firewall must also be determined after an IS1 risk assessment for the system in question).**
- **If an IPSec VPN (in accordance with CESG requirements, ask FISO) or a TLS connection is used then additional boundary control protection will be necessary at both the client and the server end. CESG advice on the required level of boundary control protection must be sought as part of the CESG approval process. It is likely that a separate evaluated firewall will be required at both the client and server ends of the connection.**

Specific Requirements for Remote Access to CONFIDENTIAL Systems

A client which connects to a CONFIDETIAL network must be protected by an ENHANCED grade whole disk encryption device when turned off/powered down.

When logging into the client device, user authentication must be carried out in accordance with CESG guidelines (contact FISO for details).

In general, an ENHANCED grade link or network encryption product is required to protect the remote access connection. HMG Infosec guidance gives full details of allowable exceptions to this requirement.

If connecting via a public IP-based network, protective measures must be put in place to guard against network attack. In addition to the ENHANCED grade link or network encryption product (which provides some boundary control protection), a separate evaluated firewall must be installed at the server end of the connection (placed between the Enhanced Grade Encryption device and the internet connection). The EAL level of the firewall must be determined after an IS1 risk assessment for the system in question. No additional boundary control protection is necessary at the client end unless this is specified in the handling instructions for the cryptographic device (in which case the EAL level of the client end firewall must also be determined after an IS1 risk assessment for the system in question.

Remote Access to SECRET and TOP SECRET Systems

Remote access to systems at these protective markings requires extremely high levels of physical and technical protective measure and is only likely to be appropriate in exceptional circumstances. Contact FISO for advice.

INDIVIDUAL ROLES AND RESPONSIBILITIES

BCU Commanders and Department Heads
Are responsible to ensure that any users within their section who need Remote Access are identified and properly managed.

ICT Department

The ICT department are responsible for ensuring that the way remote users connect to Force systems is secure and well managed in line with this policy.

Line Managers

Are responsible for ensuring that any members of their team who are accessing SWP information remotely are familiar with this policy and are complying with it.

Users

Are responsible for ensuring that they are familiar with this policy and are compliant with it.

SPECIFIC GUIDANCE – *Access Control*

PROCEDURAL HEALTH AND SAFETY CONSIDERATIONS
NONE

SPECIFIC PROCEDURES

Business Requirement for Access Control

Access to information and business processes must be controlled on the basis of business and security requirements. This must take account of policies for information dissemination and authorisation.

Policy and Business Requirements

Business requirements for access control must be defined and documented in each system Risk Management Accreditation Document Set (RMADS). Access control rules and rights for each user or group of users must be clearly stated in an access policy statement for the particular system. Users and service providers must be given a clear statement of the business requirements to be met by access controls.

The policy must take account of the following:

a. Security requirements of individual business applications;
b. Identification of all information related to the business applications;
c. Policies for information dissemination and authorisation, e.g. the need to know principle and security levels and classification of information;
d. Consistency between the access controls and information classification policies of different systems and networks;
e. Relevant legislation and any contractual obligations regarding protection of access to data or services;
f. Standard user access profiles for common categories of jobs; and
g. Management of access rights in a distributed and networked environment which recognises all types of connections available;

Access Control Rules

In specifying the access control rules, care must be taken to consider the following:

a. Differentiating between rules that must always be enforced and rules that are optimal or conditional;
b. Establishing rules based on the premise "What must be generally forbidden unless expressly permitted" rather than the weaker rule "Everything is generally permitted unless expressly forbidden";
c. Changes in information labels that are initiated automatically by

information processing facilities and those initiated at the discretion of the user;
d. Changes in user permissions are initiated automatically by the information system and those initiated by an administrator;
e. Rules which require administrator or other approval before enactment and those which do not.

User Access Management

Formal procedures are in place to control the allocation of access rights to information and services.

The procedures cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention has been given where appropriate, to the need to control the allocation of privileged access rights to override system controls.

User Registration

There is a formal user registration and de-registration procedure for granting access to all multi-user information systems and services.

Access to multi-user information services is controlled through a formal user registration process, which includes:

a. Using unique user IDs so that users can be linked to and made responsible for their actions. The use of group IDs must only be permitted where they are suitable for the work carried out;
b. Checking that the user has authorisation from the system owner for the use of the information system or service. Separate approval for access rights from management may also be appropriate;
c. Checking that the level of access granted is appropriate to the business purpose and is consistent with organisational security policy, e.g. it does not compromise segregation of duties;
d. Giving users a written statement of their access rights;
e. Ensuring service providers do not provide access until authorisation procedures have been completed;
f. Maintaining a formal record of all persons registered to use the service;
g. Immediately removing access rights of users who have changed jobs or left the organisation;
h. Periodically checking for and removing, redundant user IDs and accounts; and
i. Ensuring that, redundant user IDs are not issued to other users.

Consideration has been given to including clauses in staff contracts and service contracts that specify sanctions if unauthorised access is attempted by staff or service agents.

Privilege Management

The allocation and use of privileges (any feature or facility of a multi-user information system that enables the user to override system or application

controls) must be restricted and controlled. Inappropriate use of system privileges is often found to be a major contributory factor to the failure of systems that have been breached.

Multi-user systems that require protection against unauthorised access must have the allocation of privileges controlled through a formal authorisation process outlined in the systems RMADS.

The following steps must be considered:

a. The privileges associated with each system product, e.g. operating system, database management system and each application and the categories of staff to which they need to be allocated must be identified;
b. Privileges must be allocated to individuals on a need-to-use basis and on an event-by-event basis, i.e. the minimum requirement for their functional role only when needed;
c. An authorisation process and a record of all privileges allocated must be maintained. Privileges must not be granted until the authorisation process is complete;
d. The development and use of system routines must be promoted to avoid the need to grant privileges to users; and
e. Privileges must be assigned to a different user identity from those used for normal business use.

User Password Management

Passwords are a common means of validating a user's identity to access an information system or service. The allocation of passwords must be controlled through a formal management process, as defined by the systems RMADS.

Users must follow good security practices in the selection and use of passwords, and are expected to:

a. Keep passwords confidential;
b. Change passwords whenever there is any indication of possible system or password compromise;
c. Select quality passwords with minimum length of eight characters which are:
    1. Easy to remember;
    2. Not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers and dates of birth etc.;
    3. Free of consecutive identical characters or all-numeric or all-alphabetical groups;

d. Change passwords at regular intervals or based on the number of accesses (passwords for privileged accounts must be changed more frequently than normal passwords) and avoid re-using or cycling old passwords;
e. Change temporary passwords at first logon;
f. Do not include passwords in any automated logon process, e.g. stored in an macro or function key;
g. Do not share individual user passwords;

The protective marking applied to a password is the highest protective marking of data to which the password gives access. In systems where separation of data is not accredited this equates to the highest protective marking of data on the system.

User Responsibilities

To prevent unauthorised user access, the co-operation of users is essential for effective security. Users must be aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

Unattended User Equipment

Users must ensure that unattended equipment has appropriate protection. Equipment installed in user areas, e.g. workstations or file servers, may require specific protection from unauthorised access when left unattended for an extended period. All users and contactors must be made aware of the security requirements and procedures for protecting unattended equipment.

Users must:

a. Terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism e.g. a password protected screen saver;
b. Log-off systems and applications computers when the session is finished; and
c. Secure PCs or terminals from unauthorised use by a key lock or an equivalent control, e.g. password access, when not in use.

In addition to the above controls, departments must ensure that the appropriate security measures are taken to physically protect unattended equipment.

Network Controls

Access to both internal and external networked services must be controlled.

This is necessary to ensure that users who have access to networks and network services do not compromise the security of these network services. Such controls include:

a. Appropriate interfaces between the organisations network and network services owned by other organisations, or public networks;
b. Appropriate authentication mechanisms for users and equipment;
c. Control of user's access to information services.

Network security is concerned with the management and control of the elements (including hardware, software, information and documentation) contained within the network infrastructure. Connections between networks can be complicated by the differing security profiles of the two connecting networks and the business requirements of the connection.

Access to network infrastructure must be limited by using procedural, physical

and logical controls and supported by a Protective Monitoring policy.

All users of the network must be identified and have their identity confirmed by a suitable authentication process. The creation of false users must be prevented by the protection of the associated management functions.

Passwords provide only one level of user authentication and stronger mechanisms, such as tokens and biometrics, must be used whenever highly privileged user-ids are being protected. Passwords that are stored for use in the verification process must be protected from disclosure, modification and replay. Normally this is done by storing passwords in an encrypted form. Whenever possible, passwords must not be transmitted across networks in their plain form.

Policy on use of Network Services

Insecure connections to network services can affect the whole organisation. Users must only be provided with direct access to the services that they have been specifically authorised to use. This control is particularly important for network connections to sensitive or critical business applications or to users in high-risk locations, e.g. public or external areas that are outside the organisations security management and control.

As part of the procedure for the accreditation of our RESTRICTED domain, a network security policy is being formulated concerning the use of networks and networked services. It will cover:

a. The networks and network services which are allowed to be accessed;
b. Authorisation procedures for determining who is allowed to access which networks and networked services; and
c. Management controls and procedures to protect the access to network connections and networked services. This policy must be consistent with the business access control policy.

Enforced Path

The path from the user terminal to the computer service must be controlled. Networks are designed to allow maximum scope for a sharing of resources and flexibility of routing. These features may also provide opportunities for unauthorised access to business applications, or unauthorised use of information facilities. Controls must be incorporated that restrict the route between a user terminal and the computer services its user is authorised to access, e.g. creating an enforced path can reduce such risks.

The objective of an enforced path is to prevent any users selecting routes outside the route between the user terminal and the services that the user is authorised to access.

This usually requires the implementation of a number of controls at different points in the route. The principle is to limit the routing options at each point in the network, through predefined choices. Examples of this are as follows:

a. Allocating dedicated lines or telephone numbers;
b. Automatically connecting ports to specified applications systems or

security gateways;
c. Limiting menu and submenu options for individual users;
d. Preventing unlimited network roaming;
e. Enforcing the use of specified application systems and/or security gateways for external network users;
f. Actively controlling allowed sources to destination communications via security gateways, e.g. firewalls;
g. Restricting network access by setting up separate logical domains, e.g. virtual private networks, for user groups within the organisation.

The requirements for an enforced path are based on the ACPO/ACPOS Community Security Policy (CSP) and HMG Guidelines (such as The Manual of Protective Security).

User Authentication for External Connections

External connections provide a potential for unauthorised access to business information, e.g. access by dial-up methods. Therefore access by remote users must be subject to authentication. There are different types of authentication method, some of these provide a greater level of protection than others, e.g. method based on the use of cryptographic techniques can provide strong authentication. It is important to determine from a risk assessment the level of protection required. This is needed for the appropriate selection of an authentication method.

Currently SWP allow a limited remote access which is controlled via a secure VPN using a TACACS server. This is limited to ICT engineers and other third party contractors who may need access to these systems. The exact method of controlling remote access onto SWP systems is outlined in the CJX Accreditation Document Set held by the FISO.

A project has been initiated to allow chief officer's remote access to their SWP systems via a secure hardware token and utilises the CESG approved Cable and Wireless method for remote access. Further details can be found in the Remote Access Accreditation document also held by the FISO.

Procedural Aspects of Communications Security

Authentication

It is important to ensure that protectively marked information is only accessed by authorised persons and therefore only transmitted to the correct recipient(s). Therefore, the originator must be satisfied that they are communicating with the intended recipient and that the recipient is authorised to receive the information. Equally, the recipient must be satisfied of the validity of the originator. Users must therefore be trained and practiced in proper authentication procedures, as required and must always be suspicious of a delayed response to an authentication request.

Node Protection

A facility for authentication to a remote computer could provide a way of gaining unauthorised access to a business application. Connections to remote computer

systems must therefore be authenticated.

This is especially important if the connection uses a network outside the control of the organisations security management.

Node authentication can serve as an alternative means of authenticating groups of remote users where they are connected to a secure, shared computer facility.

Remote Diagnostic Port Protection

Access to diagnostic ports must be securely controlled. Many computers and communications systems are installed with a dial-up remote diagnostic facility for use by maintenance engineers. If unprotected these diagnostic ports provide a means of unauthorised access. They must therefore be protected by an appropriate mechanism, e.g. a key lock and a procedure to ensure that they are only accessible by arrangement between the manager of the computer service and the hardware/software support personnel requiring access.

Before these systems go 'live' a Risk Managed Accreditation Document Set (RMADS) must be produced outlining the controls for remote access for engineers.

Segregation in Networks

Networks are increasingly being extended beyond traditional organisational boundaries, as business partnerships are formed that may require the interconnection or sharing of information processing and networking facilities. Such extensions might increase the risk of unauthorised access to already existing information systems that use the network, some of which might require protection from other network users because of their sensitivity or criticality. In such circumstances the introduction of controls within the network, to segregate groups of information services, users and information systems, must be considered.

One method of controlling the security of large networks is to divide them into separate logical network domains, e.g. an organisations internal network domains and external network domains, each protected by a defined security perimeter. Such a perimeter can be implemented by installing a secure gateway between the two networks to be interconnected to control access and information flow between the two domains. This gateway must be configured to filter traffic between these domains and to block unauthorised access in accordance with the organisations access control policy.

The criteria for segregation of networks into domains must be based on the access control policy and access requirements and also take account of the relative cost and performance impact of incorporating suitable network routing or gateway technology.

Network partitioning is a powerful method of separating different communities and restricting user access within a network. It can be implemented in a number of ways:

a. Physical – this is the process of maintaining physically separate

networks or infrastructure for different systems to ensure that one does not allow unauthorised access to the other. It provides the most assured overall security but at the price of duplicated equipment and administrative overheads;

b. Logical – SWP has used a number of different techniques to achieve logical partitioning by:

Physical Address	The network defines a group of physical addresses, a subset of all the physical addresses on the network, as a community. Some networks can control which protocols may be used from a given address, for example, allowing e-mail but not file transfer.
Identifier	The network recognises different communities by the user ID. Such communities are often known as a Closed User Group and tend to be implemented by vender dependant applications.
Encryption	All users of a particular community (sometimes called a community of interest (COI)) or sub-network are equipped with encryption facilities, thereby creating a Virtual Private Network (VPN) or "tunnel". The partition is enforced by distributing keys only to the authorised members of the community.
Routers	These are network communication devices allowing or barring packets from being transmitted across sub-network boundaries. Their routing tables can be set up to control access between LANs according to either the senders or recipient's network address. These devices are not normally considered by their vendors to be security devices, but communication devices for the efficient implementation of network infrastructure.
Secure Gateways	Commonly known as Guards or Firewalls, act as bridges or routers that perform a greater level of security checking before sending on data packets across network boundaries. They act as barrier devices and are often implemented where a trusted network interfaces to an un-trusted network. It is important to realise that a Firewall is a collection of trusted devices forming an architecture that provides Firewall functionality.

Network Access Controls

Access control policy requirements for shared networks, especially those extending across organisational boundaries, require the incorporation of controls to restrict the connection capability of the users. Such controls can be implemented through network gateways that filter traffic by means of pre-defined tables or rules. The restrictions applied must be based on the access policy (as outlined in the systems accreditation document) and requirements of the business application and must be maintained and updated accordingly.

Examples of applications to which restrictions must be applied to are:

a. Electronic mail;

b. One-way file transfer;
c. Both-ways file transfer;
d. Interactive access;
e. Network access linked to a time of day or date;
f.

Network Routing Control

Shared networks, especially those extending across organisational boundaries, require the incorporation of routing controls to ensure that computer connections and information flows do not breach the access control policy of the business applications. This control is often essential for networks shared with third party users.

Routing controls must be based on positive source and destination address checking mechanisms. Network address translation is also a very useful mechanism for isolating networks and preventing routing to propagate form the network of one organisation to another. They can be implemented in software or hardware. Implementers must be aware of the strength of any mechanisms deployed.

The CJX Code of Connection requires SWP to ensure that any extending connections across organisational boundaries (for example 101 SNEN) are protected by an EAL4 Firewall configured to CESG Standards. For more information please contact the FISO on 20-954 or 20-682.

Security of Network Services

All protectively marked information communicated across a network must be encrypted. The grade of encryption is always linked to the protective marking of the information. The encryption standard for protectively marked information is as follows:

- **RESTRICTED requires Baseline Grade**
- **CONFIDENTIAL and short term SECRET requires Enhanced Grade**
- **Long Term SECRET and TOP SECRET requires High Grade.**

There may be occasions where these controls are not suitable because of operational reasons; this will need to be outlined in the Accreditation document for the system and the Senior Information Risk Owner (ACC Specialist Operations) will make the final decision after assessing the risk of compromise to the Force.

Operating System Access Control

Security facilities at the operating system level must be used to restrict access to computer resources. These facilities must be capable of the following:

a. Identifying and verifying the identity and if necessary the terminal or location of each authorised user;
b. Recording successful and failed system accesses;
c. Providing appropriate means for authentication, if a password management system is used. It must ensure quality passwords;
d. Where appropriate, restricting the connection times of users;

Other access control methods, such as challenge-response, are available if these are justified on the basis of business risk.

Automatic Terminal Identification

Automatic terminal identification must be considered to authenticate connections to specific locations and to portable equipment. Automatic terminal identification is a technique that can be used if it is important that the session can only be initiated from a particular location or computer terminal. An identifier in or attached to, the terminal can be used to indicate whether this particular terminal is permitted to initiate or receive specific transactions. It may be necessary to apply physical protection to the terminal, to maintain the security of the terminal identifier. A number of other techniques can also be used to authenticate users.

Terminal Logon Procedures

Access to information services must be attainable via a secure log-on procedure. The procedure for logging onto a computer system must be designed to minimise the opportunity for unauthorised access. The log-on procedure must therefore disclose the minimum information about the system, in order to avoid providing an unauthorised user with unnecessary assistance. A good log-on procedure must:

a. Not display system or application identifiers until the log-on process has been successfully completed;
b. Display a general notice warning that the computer must only be accessed by authorised users;
c. Not provide help messages during the log-on procedure that would aid an unauthorised user;
d. Validate the log-on information only on completion of all input data. If an error condition arises, the system must not indicate which part of the data is correct or wrong;
e. Limit the number of unsuccessful log-on attempts allowed (three is recommended) and consider:

    1. Recording unsuccessful attempts;
    2. Forcing a time delay before further log-on attempts are allowed or rejecting any further attempts without specific authorisation;
    3. Disconnecting data link connections;

f. Limit the maximum and minimum time allowed for the log-on procedure. If exceeded, the system must terminate the log-on;
g. Display the following information on completion of a successful log-on:
    1. Date and time of the previous successful attempt;
    2. Details of any unsuccessful log-on attempts since the last successful log-on;

User Identification and Authentication

All users (including technical support staff, such as operators, network administrators, system programmers and database administrators) must have a unique identifier (user ID) for their personal and sole use so that activities can

subsequently be traced to the responsible individual. User IDs must not give any notification of the user's privilege level, e.g. manager, supervisor.

In exceptional circumstances, where there is a clear business benefit, the use of a shared user ID for a group of users or a specific job can be used. Approval by management must be documented for each case. Additional controls may be required to maintain accountability.

There are various authentication procedures, which can be used to substantiate the claimed identity of a user. Passwords are a very common way to produce identification and authentication based on a secret that only the user knows. The same can also be achieved with cryptographic means and authentication protocols.

Objects such as memory tokens or smart cards that users possess can also be used for Identification and Authentication. Biometric authentication technologies that use the unique characteristics or attributes of an individual can also be authenticating the person's identity. A combination of techniques and mechanisms securely linked will result in stronger authentication.

Password Management System

Passwords are one of the principle means of validating a user's authority to access a computer service. Password management systems must provide an effective, interactive facility, which ensures quality passwords.

Some applications require user passwords to be assigned by an independent authority. In most cases the passwords are selected and maintained by users. A good password management system must:

a. Enforce the use of individual passwords to maintain accountability;
b. Where appropriate allow users to select and change their own passwords and include a confirmation procedure to allow for input errors;
c. Enforce a choice of quality passwords;
d. Where users maintain their own passwords, enforce password changes regularly;
e. Where users select passwords, force them to change temporary passwords at first log-on;
f. Maintain a record of previous user passwords, e.g. for the previous 12 months and prevent re-use;
g. Not display passwords on the screen when being entered;
h. Store passwords files separately form application system data;
i. Store passwords in encrypted from using a one-way encryption algorithm;
j. Alter default vendor passwords following installation of software;

Use of System Utilities and Potentially Harmful Software

Most computer installations have one or more system utility programs that might be capable of overriding system and application controls. There may also be a requirement for certain other system and network monitoring tools to be installed. It is essential that their use is restricted and tightly controlled. The

following controls must be considered:

a. Only duly authorised ICT personnel are allowed to system utilities;
b. System utilities must be segregated from application software;
c. Any use of system utilities by personnel other than ICT must have prior written approval from FISO.
d. All use of system utility tools must be logged appropriately;
e. ICT must document the use and authorisation levels of system utilities;
f. Removal of all unnecessary software based utilities and system software on computer builds, prior to deployment;

Terminal Time-out

Inactive terminals in high risk locations, e.g. public or external areas outside the organisations security management, or serving high risk systems, must shut down after a defined period of inactivity to prevent access by unauthorised persons. This time-out facility must clear the terminal screen and close both application and network sessions after a defined period of inactivity. The time-out delay must reflect the security risks of the area and the users of the terminal.

A limited form of terminal time-out facility can be provided for some PCs which clear the screen and prevents unauthorised access but does not close down the application or network sessions.

Limitations of Connection Time

Restrictions on connection times must provide additional security for high-risk applications. Limiting the period during which terminal connections are allowed to computer services reduce the window of opportunity for unauthorised access. Such a control must be considered for sensitive computer applications, especially those with terminals installed in high risk locations, e.g. public or external areas that are outside the organisations security arrangement.

Examples of such restrictions include:

a. Using predetermined time slots, e.g. for batch file transmissions, or regular interactive sessions of short duration;
b. Restricting connection times to normal office hours if there is no requirement for overtime or extended-hours operation;

Application Access Control

To prevent unauthorised access to information held in information systems, security facilities must be used to restrict access within application systems. Logical access to software and information must be restricted to authorised users. Application systems must:

a. Control user access to information and application system functions, in accordance with a defined business access control policy;
b. Provide protection from unauthorised access for any utility and operating system software that is capable of overriding system or application controls;

c. Not compromise the security of other systems with which information resources are shared;
d. Be able to provide access to information to the owner only, other nominated authorised individuals, or defined groups of users;

Information Access Restriction

Users of application systems, including support staff, must be provided with access to information and application system functions in accordance with a defined access control policy, based on individual business application requirements and consistent with organisational information access policy. Application of the following controls must be considered in order to support access restriction requirements:

a. Providing menus to control access to application systems functions;
b. Restricting users knowledge of information or application system functions which they are not authorised to access, with appropriate editing of user documentation;
c. Controlling the access rights of users, e.g. read, write, delete and execute;
d. Ensuring that outputs from application systems, handling sensitive information contain only the information that is relevant to the use of the output and is sent only to authorised terminals and locations, including periodic review of such outputs to ensure their redundant information is removed.

Sensitive System Isolation

Sensitive systems might require a dedicated (isolated) computing environment. Some application systems are sufficiently sensitive to potential loss that they require special handling. The sensitivity may indicate that the application system must run on a dedicated computer, must only share resources with trusted application systems, or have no limitations. The following considerations apply:

a. The sensitivity of an application system must be explicitly identified and documented by the application owner;
b. When a sensitive application is to run in a shared environment, the application systems with which it will share resources must be identified and agreed with the owner of the sensitive application;

Protective Monitoring

Systems must be monitored to detect deviation from access control policy and record significant events to provide evidence in case of security incidents.

System monitoring allows the effectiveness of controls adopted to be checked and conformity to an access policy model to be verified.

SWP has invested in an auditing product which monitors user's actions on the network; this is controlled via Professional Standards.

Accounting

Audit logs recording exceptions and other security relevant events must only be produced and kept for an agreed period to assist in future investigations and access control monitoring. Audit logs must also include:

a. User IDs;
b. Dates and times for log-on and log-offs;
c. Terminal identity or location if possible;
d. Records of successful and rejected system access attempts;
e. Records of successful and rejected data and other resource access attempts. Certain audit logs may be required to be achieved as part of the record retention policy or because requirements to collect evidence.

Once an information system is in use, it is essential for security management personnel to be able to track the way in which the system is used and to ensure that security controls are effective in practice. Specific events and details relating to the operation of the system and its security controls must be recorded for subsequent inspection and analysis. This process is called Protective Monitoring. More than other forms of security, information security measures are liable to be influenced by technology developments and re-configuration and regular audit review is essential.

Monitoring System Use

Procedures and Areas of Risk

Procedures for monitoring use of information processing facilities must be established. Such procedures are necessary to ensure that users are only performing activities that have been explicitly authorised. The level of monitoring required for individual facilities must be determined by a risk assessment.

Areas that must be considered include:

a. Authorised access, including details such as:

    1. The user ID;
    2. The date and time of key events;
    3. The types of events;
    4. The files accessed;
    5. The program/utilities used;

b. All privileged operations, such as:
    a. Console alerts or messages;
    b. System log exceptions;
    c. Network management alarms;

In addition to the above controls, departments must also consider communications security Defensive Monitoring, to ensure compliance with Comsec policy and enable subsequent detection of Comsec incidents. This service to provide damage limitation, education and policy response.

Risk Factors

The result of the monitoring activities must be reviewed regularly. The frequency of the review must depend on the risks involved. Risk factors that must be considered include:

a. The criticality of the application processes;
b. The value, sensitivity or criticality of the information involved;
c. The past experience of system infiltration and misuse;
d. The extent of system interconnection (particularly public networks);

Logging and Reviewing Events

A log review involves understanding the threats faced by the system and the manner in which these may arise. Examples of events that might require further investigation in case of security incidents are given above under Accounting.

System logs often contain a large volume of information, much of which is extraneous to security monitoring. To help identify significant events for mobile phones, special care must be taken to ensure that business information is not compromised. A formal policy has been adopted that takes into account the risks of working with mobile computer facilities, in particular in unprotected environments.

When allocating the responsibilities for log review, a separation of roles must be considered between the person(s) undertaking the review and those whose activities are being monitored.

Particular attention must be given to the security of the logging facilities because of tampered with it can provide a false sense of security. Controls must aim to protect against unauthorised changes and operational problems including:

a. The logging facilities being de-activated;
b. Alterations to the messages types that are recorded;
c. Log files being edited or deleted;
d. Log files media becoming exhausted and either failing to record events or over-writing itself;

Clock Synchronisation

The correct setting of computer clocks is important to ensure accuracy of audit logs, which may be required for investigation or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence.

Where a computer or communication device has the capability to operate a real-time clock, it must be set to an agreed standard, e.g. Universal Co-ordinated Time (UCT) or local standard time. As some clocks are known to drift with time there must be a procedure that checks for and corrects any significant variation.

Those responsible for any UK HMG Computer and/or network environment requiring an accurate and nationally consistent time, be it for Protective Monitoring purposes or other, must ensure that the product they select to deliver

this takes its source from the British MSF Time Signal Transmitter, transmitted by the national Physics Laboratory.

INDIVIDUAL ROLES AND RESPONSIBILITIES

System Owners

Must ensure that the access controls are suitable for the protective marking of the data which is being processed or stored by the system.

There must be a formal registration/de-registration process in place for granting access and revoking access to the system.

It is the responsibility of the System Owner to authorise new users on the system, this can be done, either by themselves personally or by another person or unit, given suitable delegated authority. This delegated authority will handle the day-to-day administration of the system, but the responsibility will remain with the designated System Owner.

Force Information Security Officers (FISO's)

Are responsible for advising the System Owner on suitable controls for the system and conducting security audits to ensure compliance.

FISO's are responsible for ensuring that any security breaches in relation to access control are reported to CESG.

FISO's are also responsible for keeping a record of breaches involving unauthorised access to systems and SWP premises as well as any remedial action taken.

Assistant Director CITD

Must ensure that all ICT are appropriately vetted for their role and that the access given to them is only as much as they need to fulfil their assigned role.

The actions taken by ICT staff must be fully auditable on the system. It is also the AD/CITD responsibility to ensure that in the event of any member of ICT staff being involved in an information security breach, the persons account is suspended, during an investigation.

Any security breach, which is department becomes aware of, must be reported to the FISO at the earliest opportunity.

It is the responsibility to ensure that there is adequate monitoring and logging of activity on the ICT Infrastructure.

Users

To prevent unauthorised user access, the cooperation of users is essential for effective security. Users must make themselves aware of the FISP and the security policies for the various systems which they use.

Users are responsible for any actions performed under there account, so this must be taken into consideration when deciding whether to share their passwords with others (which incidentally is a serious breach of FISP and could result in disciplinary action be taken).

The user must contact FISO if they believe that there account has been compromised, or if they become aware of any other security breach.

SOUTH WALES POLICE
FORCE POLICIES & PROCEDURES

SPECIFIC GUIDANCE – *Acceptable Use*

PROCEDURAL HEALTH AND SAFETY CONSIDERATIONS
NONE

SPECIFIC PROCEDURES

Introduction

The intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to SWP established culture of openness, trust and integrity. SWP is committed to protecting SWP employees, partner's agencies from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail and WWW browsing are the property of SWP. These systems are to be used for business purposes in serving the interests of SWP in performance of our duties to the public.

Effective security is a team effort involving the participation and support of every SWP employee and partner who deals with information and /or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment in SWP. These rules are in place to protect the employees and SWP. Inappropriate use exposes SWP to risks including virus attacks, compromise of networks and services and legal issues.

Scope

This policy applies to employees, contractors, consultants, temporary staff and other workers at SWP premises including all personnel affiliated with third party (partner) agencies. This policy applies to al equipment that is owned or leased by SWP.

Policy

1. While SWP ICT desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of SWP. Because of the need to protect SWP's network, management cannot guarantee the confidentiality of information stored on any network device belonging to SWP.
2. SWP provides access to Internet/Intranet and Extranet facilities. These facilities are only to be used for business related purposes.

3. For security and network maintenance purposes, authorised individuals within SWP monitor equipment, systems and network traffic at any time.
4. SWP reserve the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Propriety Information

1. All information held or processed by SWP is regulated by the Government Protective Marking Scheme (GPMS) as outlined in above guidance. Any access to SWP information must be authorised and given on a 'need to know' basis to properly authorised and vetted personnel. Any disclosure to non authorised persons or persons not vetted to the appropriate level will be considered a violation of this policy and could lead to disciplinary action being taken by Professional Standards.
2. Keep passwords secure and do not share accounts. Authorised users are responsible for the security of their passwords and accounts. System level passwords must be changed quarterly, users level passwords should be changed every month.
3. All PC's laptops and workstations must b secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging off (control-alt-delete, for Windows) when the PC is left unattended.
4. Encryption must be compliant with CESG guidelines as laid out in the HMG Security Policy Framework (SPF).
5. Users must not post e-mails on social network sites, using their Force e-mails and should be careful of identifying themselves as SWP employees. Any postings which identify the individual as SWP employee, must comply with this Force policy.
6. Users must not set up social network sites branded with SWP, unless specifically authorised to do so by their Head of Department and FISO. Any employee that ignores this requirement will be liable for disciplinary action by Professional Standards.
7. Users are NOT allowed to connect any non-SWP issue ICT device into the SWP network, unless specific approval has been given by the Head of Department, Assistant Director Corporate Information & Technology and FISO.
8. All users must use extreme caution when opening e-mail attachments received from unknown senders, as they may contain viruses, e-mail bombs or Trojan horse code.

Unacceptable Use

The following activities are prohibited unless they perform these activities as a part of their legitimate job responsibilities. (For example ICT staff).

Under no circumstances is an employee of SWP authorised to engage in any activity that is illegal under UK law, while utilising SWP owned resources.

The list below is by no means exhaustive, but attempts to provide a framework for activities which fall into the category of unacceptable use.

Systems and Network Activities

The following activities are strictly prohibited:

1. Users are not allowed to install any software on their PC, without prior approval from Assistant Director CI&T and FISO.
2. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws and regulations, including but not limited to the installations or distribution of "pirated" or other software products that are not appropriately licensed for use by SWP.
3. Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from, books, or other copyrighted sources, copyrighted music and the installation of any copyrighted software for which SWP or the end user does not have an active license is strictly prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The FISO must be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g. viruses. worms, Trojan horses, e-mail bombs, etc.).
6. Using a SWP computing asset to actively engage in procurement or transmitting material that is in violation of sexual harassment or hostile workplace laws.
7. Storing, processing copying or distributing pornographic material is strictly prohibited, unless it is in line with the individuals role and they have suitable authorisation from their Head of Department.
8. Revealing your account password to others, or allowing use of your account by others.
9. Effecting security breaches or disruptions of network communications. Security breaches include but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section "disruption" includes but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification is given to FISO and approval is sought from the Assistant Director CI&T.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example denial of service attack).
14. Using any program/script/command or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

E-mail and Communications Activities

The following activities are strictly prohibited:

1. Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via e-mail, telephone or paging, whether through language, frequency or size of message.
3. Unauthorised use or forging of e-mail header information.
4. Creating or forwarding of "chain letters", "Ponzi" or other "pyramid" schemes of any type.
5. Sending an e-mail Force broadcast without proper authorisation. For example sending out an e-mail to everyone in your department or BCU, without prior approval from your Head of Department or BCU Commander.

For more information please see the specific guidance on E-mail and Internet use.

Social Networking sites

The following is strictly prohibited:

1. Setting up an "official" social network site for SWP, without first seeking approval from the Information Security Board (ISB) and Corporate Communications.
2. Posting any offensive, illegal or inflammatory material.
3. Discussing any work related or protectively marked material above PROTECT on a social site or forum.

INDIVIDUAL ROLES AND RESPONSIBILITIES

BCU Commanders and Department Heads

It is the BCU Commanders and Department Heads responsibility to ensure that everyone in their BCU or Department is aware and understands the requirements of the Acceptable Use Policy.

Line Managers

It is the line manager's responsibility to ensure that everyone in their unit is familiar with the Acceptable Use Policy.

Users

Users are responsible for ensuring that they comply with this policy.

IMPLICATIONS OF THE POLICY
Financial implications/best value
The financial costs of implementing this policy will include the introduction of systems such as business continuity and disaster recovery systems, as well as changes to processes and procedures within the force. In particular the introduction of the Government Protective Marking Scheme (GPMS) will involve some financial cost in enabling staff to protectively mark documents. The need for a force wide confidential network for applications that hold a protective marking of CONFIDENTIAL will involve a substantial financial investment in both money and resources. The introduction of these systems is critical for IMPACT and Unified Police Security Architecture (UPSA).
Human resources/training
Certain elements within the policy will involve changes in the way staff perform there day to day work, the most obvious of these being the introduction of the Government Protective Marking Scheme (GPMS) which will force staff to apply a protective marking to every document that they or their department produce. This will have training costs, which could be included in the IMPACT program budget, as it is a deliverable of the IMPACT program.
Annual plan links
Partnership links
Assessed Risks

SOUTH WALES POLICE
FORCE POLICIES & PROCEDURES

Handling Protectively Marked Material

A Guide for Police Personnel

Revised April 2007

Introduction

The Chief Constables' Council originally mandated adoption of the Government Protective Marking Scheme in 2001. This is now a formal compliance requirement of the ACPO/ACPOS Information Systems Community Security Policy.

This guidance leaflet supersedes and replaces the previous issue dated October 2001.

Personnel need to be aware that it is important that protective security practices:

- Implement the 'need to know' principle
- Are workable and user-friendly
- Deal with all the prevailing threats
- Are effectively co-ordinated by the Personnel who use them
- Are just, open and reasonable, where they may impinge on the lives of staff

When selecting the appropriate marking, personnel should also consider:

- How damaging the consequences would be if material was lost, stolen, disclosed or destroyed
- Correct marking is applied (over or under classification damages the credibility of the system)
- A compilation of many items marked at the same level may require the whole to be marked at a higher level
- The scheme should not be used to protect against sensitivities likely to arise due to inefficiency or administrative error
- It does not provide exemption from Freedom of Information legislation
- Regular reviews of the material may be necessary in order to downgrade or destroy any such material

As from February 2007 there are now five levels of Protective Marking* that can be applied to sensitive assets, depending on the degree of sensitivity involved:

1. PROTECT
2. RESTRICTED
3. CONFIDENTIAL
4. SECRET
5. TOP SECRET

The majority of information held within the Police Service contains personal or sensitive data and therefore requires a level of Protective Marking.

(Information already in the public domain will not require a protective mark.)

This guide predominantly deals with assets that are marked at either PROTECT, RESTRICTED or CONFIDENTIAL, as they comprise the vast majority of 'sensitive' information assets held within the Police Service.

It is intended to give very basic guidance on the application of protective markings to **police information** together with storage handling and movement requirements.

It is not exhaustive! For further clarification and in particular for advice regarding SECRET and TOP SECRET please contact your Information Security Officer.

**NB – When used as a Protective Marking – the words PROTECT / RESTRICTED / CONFIDENTIAL / SECRET and TOP SECRET, will be displayed in capitals to differentiate them from ordinary use within documents.*
The same rule applies when attaching a descriptor (see later) all DESCRIPTORS will be written in capital letters.

Impact Criteria – Public Order, Public Safety and Law Enforcement

PROTECT

Impact Levels 1 & 2

Would accidental or deliberate compromise of assets marked **PROTECT** be likely to cause:

Impact Level 1
- No impact on life and safety;
- Minor disruption to emergency service activities that requires reprioritisation at local (station) level to meet expected levels of service;
- No impact on crime fighting;
- No impact on judicial proceedings;

Impact Level 2
- Inconvenience or cause discomfort to an individual;
- Minor disruption to emergency service activities that requires reprioritisation at area / divisional level to meet expected levels of service;
- Minor failure in local Magistrates Courts

NOTE

- PROTECT is not a national security protective marking and the policy relating to the use of RESTRICTED remains unchanged.
- Not to be used for operational issues.
- **Must** be accompanied by a Descriptor, (e.g. PROTECT – STAFF).

RESTRICTED

Impact Level 3

Would accidental or deliberate compromise of assets marked **RESTRICTED** be likely to cause:

- A risk to an individual's personal safety or liberty
- Disruption to emergency service activities that requires reprioritization at the County or organizational level to meet expected levels of service
- Hinder the detection, impede the investigation of, or facilitate the commission of low level crime (i.e. crime not defined in legislation as "serious crime"), or hinder the detection of serious crime
- A low-level criminal prosecution to collapse; cause a conviction for a low-level criminal offence to be declared unsafe or referred for appeal
- A breach of proper undertakings to maintain the confidence of material provided by third parties;
- A breach of statutory restrictions on disclosure of material (does not include the Data Protection Act 1998, where non-sensitive information is involved);
- An undermining of confidence in public services;

CONFIDENTIAL

Impact Level 4

Would accidental or deliberate compromise of assets marked **CONFIDENTIAL** be likely to cause:

- A risk to a group of individuals safety or liberty;
- Disruption to emergency service activities that requires reprioritization at national level (e.g. one police force requesting help from another) to meet expected levels of service;
- Impeding of the investigation of, or facilitate the commission of serious crime (as defined in legislation);
- A serious crime prosecution to collapse; cause a conviction for a serious criminal offence to be declared unsafe or referred to appeal;

SECRET

Impact Level 5

Would accidental or deliberate compromise of assets marked **SECRET** be likely to cause:

- A threat to life directly leading to limited loss of life;
- Disruption to emergency service activities that requires emergency powers to be invoked (e.g. military assistance to the emergency service) to meet expected levels of service;
- Major, long term impairment to the ability to investigate serious crime (as defined in legislation);
- A number of criminal convictions to be declared unsafe or referred to appeal (e.g. through persistent and undetected compromise of an evidence-handling system);

TOP SECRET

Impact Level 6

Would accidental or deliberate compromise of assets marked **TOP SECRET** be likely to:

- Lead directly to widespread loss of life;
- Threaten directly the internal stability of the UK or friendly countries leading to widespread instability;
- Cause major, long term impairment to the ability to investigate serious organised crime (as defined in legislation);
- Cause the collapse of the UK Judicial system;

'Protective Marking' is the method by which the ***originator*** of an asset (that is all material assets, ie papers, drawings, images, disks and all forms of electronic data records), indicates to others, the levels of protection required when handling the asset in question, in terms of its sensitivity, security, storage, movement both within and outside the originator's own department or force and its ultimate method of disposal.

When a protective marking is applied to an information asset it is indicating its value in terms of the damage that is likely to result from that information being compromised. The sections on this page detail the criteria **specific to public order, public safety and law enforcement** for each level of Protective Marking.

Impact Criteria – Defence, International Relations and Intelligence

PROTECT

Impact Levels 1 & 2

Would accidental or deliberate compromise of assets marked **PROTECT** be likely to cause:

Impact Level 1

- Delay or loss of minor supply service;

Impact Level 2

- Inconvenience or cause discomfort to an individual;
- The loss of a number of minor supply services;

RESTRICTED

Impact Level 3

Would accidental or deliberate compromise of assets marked **RESTRICTED** be likely to cause:

- A risk to an individual's personal safety or liberty;
- Minor loss of confidence in Government;
- More difficulty to maintain the operational effectiveness of security of UK or allied forces (e.g. compromise of UK forces doctrine or training materials);
- Embarrassment to Diplomatic relations;
- Disadvantage to a major UK company;
- Damage to unique intelligence operations in support of intelligence requirements at JIC Priority Three or less;

CONFIDENTIAL

Impact Level 4

Would accidental or deliberate compromise of assets marked **CONFIDENTIAL** be likely to cause:

- A risk to a group of individuals safety or liberty;
- Major loss in confidence in Government;
- Damage to the operational effectiveness of security of UK or allied forces (e.g. compromise of a logistics system causing re-supply problems without causing risk to life);
- Disadvantage to a number of major UK Companies;
- A halt in unique intelligence operations in support of intelligence requirements at JIC Priority Three or less, or damage unique intelligence operations in support of intelligence requirements at JIC Priority Two;

SECRET

Impact Level 5

Would accidental or deliberate compromise of assets marked **SECRET** be likely to cause:

- A threat to life directly leading to limited loss of life;
- A direct threat to the internal political stability of the UK or friendly countries;
- Severe damage to the operational effectiveness or security of UK or allied forces (e.g. compromise of the operational plans of units of company size or below in a theatre of military operations);
- A rise in international tension, or seriously damage relations with friendly governments;
- Disadvantage to the UK in international negotiations (e.g. advance compromise of UK negotiation strategy or acceptable outcomes, in the context of a bilateral trade dispute);
- A halt in unique intelligence operations in support of intelligence requirements at JIC Priority Two, or damage unique intelligence operations in support of intelligence requirements at JIC Priority One;

TOP SECRET

Impact Level 6

Would accidental or deliberate compromise of assets marked **TOP SECRET** be likely to:

- Lead directly to widespread loss of life;
- The collapse of internal political stability of the UK or friendly countries
- Cause exceptionally grave damage to the operational effectiveness or security of UK or allied forces (e.g. compromise of the operational plans of units of battalion size or above in a theatre of military operations)
- Directly provoke international conflict, or cause exceptionally grave damage to relations with friendly governments
- Severely disadvantage the UK in international negotiations (e.g. advance compromise of UK negotiation strategy or acceptable outcomes, in the context of a major EU or WTO negotiating round)
- Halt unique intelligence operations in support of intelligence requirements at JIC Priority One.

Impact Criteria – Critical National Infrastructure

PROTECT

Impact Levels 1 & 2

Would accidental or deliberate compromise of assets marked **PROTECT** be likely to cause:

Impact Level 1

- Local loss of telecoms for a few hours;
- Local power outages causing disruption for up to 12hours;
- Minimal impact on finance (less than £10,000);
- Minor disruption of a key local transport systems for up to 12 hours
- The breakdown of local water supplies and/or sewage service for a small number (<10) of people for more than a day;
- Local disruption to the distribution of some essential goods, fuel, raw materials, medicines and/or food of up to a week;

Impact Level 2

- Local loss of telecoms for up to 12 hours;
- Local power outage causing distribution for up to 24hours;
- Minor loss to a Financial Company (less than £1 million);
- Minor disruption of key local transport systems for up to 24 hours;
- The breakdown of local water supplies and/or sewage service for a small number (<50) of people for more than a week;
- Local disruption to the distribution of some essential goods, fuel, raw materials, medicines and/or disruption of food for up to a month;

RESTRICTED

Impact Level 3

Would accidental or deliberate compromise of assets marked **RESTRICTED** be likely to cause:

- Local loss of telecoms for up to 24 hours;
- Loss of power in a region causing disruption for up to 24 hours;
- Major loss of a Leading Financial company of £millions;
- Disruption of a number of key local transport systems for up to 24 hours;
- Breakdown of local water supplies and/or sewage service for a number (up to 100) of people or prolonged drought (up to 1 months);
- Regional disruption to the distribution of some essential goods, fuel, raw materials and medicines and/or widespread disruption of food for up to a week;

CONFIDENTIAL

Impact Level 4

Would accidental or deliberate compromise of assets marked **CONFIDENTIAL** be likely to cause:

- Loss of telecoms of a region for up to 24 hours;
- Loss of power in a region causing disruption for up to a week;
- Major loss of a Leading Financial Company of £10s millions;
- Major disruption of key regional transport systems for up to a week;
- Breakdown of local water suppliers and/or sewage service for over 100 people or prolonged drought (up to 1 month);
- Regional disruption to the distribution of some essential goods, fuel, raw materials and medicines and widespread disruption of food for up to a month;

SECRET

Impact Level 5

Would accidental or deliberate compromise of assets marked **SECRET** be likely to cause:

- Loss of telecoms nationally for up to a week;
- Loss of power in a region causing distribution for more than 1 week;
- Severe losses to UK Business of up to £1 billion;
- Severe national disruption of key transport systems for up to a week;
- Breakdown of regional water suppliers and/or sewage service (effecting >100 people) or prolonged drought (up to 3 months);
- National disruption to the distribution of essential goods, fuel, raw materials and medicines and widespread disruption of food for up to a month;

TOP SECRET

Impact Level 6

Would accidental or deliberate compromise of assets marked **TOP SECRET** be likely to cause:

- Loss of telecoms nationally for more than 1 week;
- Loss of power nationally affecting the whole of the UK for more than 1 week;
- Severe financial losses to UK Business of £10s billions;
- Severe national disruption of key transport systems for over a month;
- Total breakdown of national water supplies and/or sewage service (effecting >100 people) or prolonged drought (> 6 months);
- National disruption to the distribution of essential goods, fuel, raw materials and medicines and widespread disruption of food for over a month;

Handling, Storage and Movement

Application / Activity	PROTECT	RESTRICTED	CONFIDENTIAL
Marking documents	Top and bottom of every page	Top and bottom of every page	Top and bottom of every page
Storage of hard copy documents	Protected by one barrier, e.g. a locked container within a secure building.	Protected by one barrier, e.g. a locked container within a secure building.	Protected by **two** barriers e.g. a locked container in a locked room, within a secure building.
Disposal of paper waste	Use secure waste sacks. **Keep secure when left unattended.**	Use secure waste sacks. **Keep secure when left unattended.**	Use a SEAP approved cross cut shredder. **Keep secure when left unattended.**
Disposal of magnetic media	Securely destroy. Floppy disk - dismantle and cut disk into quarters & dispose with normal waste. Optical Media - destroy completely - disintegrate, pulverise, melt or shred. Use approved contractor for bulk items.	Securely destroy. Floppy disk - dismantle and cut disk into quarters & dispose with normal waste. Optical Media - destroy completely - disintegrate, pulverise, melt or shred. Use approved contractor for bulk items.	Securely destroy. Floppy disk - dismantle and cut disk into quarters & dispose with normal waste. Optical Media - destroy completely - disintegrate, pulverise, melt or shred. Use approved contractor for bulk items.
Reuse of Media (Hard Drives etc)	Triple overwrite using CESG approved software.	Triple overwrite using CESG approved software.	Triple overwrite using CESG approved software.
Movement within Force using own internal distribution system	In a sealed envelope with protective marking shown. A transit envelope **may** be used if sealed with a security label.	In a sealed envelope with protective marking shown. A transit envelope **may** be used if sealed with a security label.	In a new sealed envelope with protective marking shown. Transit envelopes **must not** be used.
Movement between forces/partner agencies	By post or courier, in a sealed envelope. **Do not show** protective marking on the envelope.	By post or courier, in a sealed envelope. **Do not show** protective marking on the envelope.	By post or courier. Double enveloped both fully addressed. Protective marking shown on inner envelope only. Return address on **outer** envelope.
Force Internal 'Phone Network	May be used.	May be used if private secure network.	May be used if private secure network in cases of operational urgency.
Public Telephone, Mobile Telephone and WAP 'phone networks	May be used.	May be used in cases of operational urgency if due caution is exercised.	Not to be used.
Pager Systems & SMS	May be used.	Not to be used.	Not to be used.
Facsimile Machines	May be used.	May be used in cases of operational urgency if due caution is exercised.	Not to be used unless encrypted fax service available.
Airwave Radios	May be used.	May be used.	Not to be used unless enhanced end to end encryption service deployed.
Force Data Network, Email Services using PNN – GSI – CJSM – MOD secure addressing conventions	May be used.	May be used.	Not to be used without encryption service compliant with ACPO/ACPOS Community Security Policy.
Internet Email / Internet Services	May be used	Not to be used without encryption service compliant with ACPO/ACPOS Community Security Policy.	Not to be used without encryption service compliant with ACPO/ACPOS Community Security Policy.

If there is a requirement to use any of the above methods of communication at a higher level than recognized safe to do so, the operational urgency and the need for transmission must be weighed against the risk of a security breach, for which the force may be held accountable. If it is decided that such transmissions are essential, they should be kept short and guarded speech used. The use of some form of prearranged codes should be considered to avoid identifying officers, informants or locations.

Requirements and restrictions on the handling/disposal etc of SECRET and TOP SECRET material are not included in this aide-memoire. Should you find yourself confronted with or required to deal with such material, seek advice or assistance from your force Information Security Officer, who will be able to advise you accordingly.

Descriptors

When you originate material requiring a Protective Marking, you ***may,*** if necessary, add a DESCRIPTOR where it ***helps indicate to others*** the nature of the sensitivity and the groups of people who need access.

One exception is the PROTECT marking which should always be used with a DESCRIPTOR from the following list:

APPOINTMENTS
Concerning actual or potential appointments that have not yet been announced

HONOURS
Unannounced recognition for exceptional Achievement

MANAGEMENT
Policy and planning affecting the interest of groups of staff

MEDICAL
Medical reports, records and material relating to staff

PERSONAL
Material intended for the person to whom it may be addressed

STAFF
Concerning references to named or identifiable staff or personal confidences entrusted by staff to management

DESCRIPTORS that can be used with either PROTECT or RESTRICTED include:

COMMERCIAL
Relating to a commercial establishments processes or affairs

CONTRACTS
Concerning tenders under consideration and the terms of any tenders

INVESTIGATIONS
Concerning investigations into disciplinary or criminal matters, involving members of the police service

PRIVATE
For information collected through electronic government services provided to the public and agencies and relating to the individual or agencies

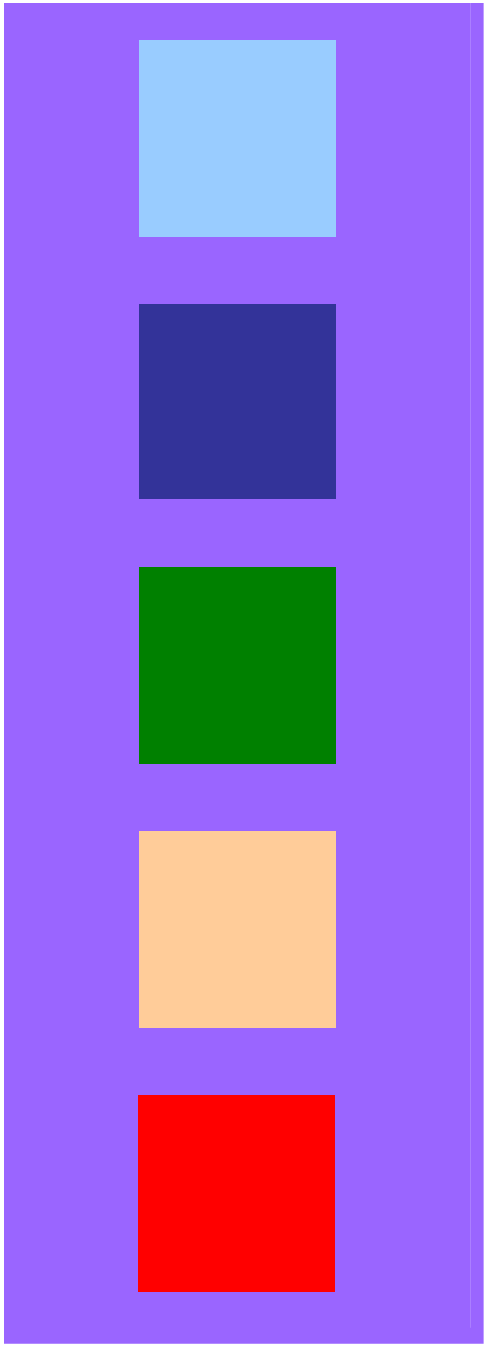
Other DESCRIPTORS include:

POLICY
Proposals for new or changed force policy, prior to publication

VISITS
Concerning details of visits by, for example, royalty, ministers and other dignitaries.

CHIS
(Covert Human Intelligence Source) regarding informants and their handling. Any informant related information should be protectively marked CONFIDENTIAL as a baseline, with the appropriate handling procedures. Information which identifies an informant should be marked SECRET

With the exception of PERSONAL or PRIVATE, which may be used by themselves, the above descriptors may only be used in conjunction with a protective marking.
Special handling instructions may also take the form of caveats, nicknames and code words or exceptionally other handling instructions e.g. DESCRIPTOR may take the form of an operation name – such as - “OPERATION RAINBOW”– EYES ONLY.



This leaflet is designed to inform staff of procedures and help them determine and indicate to others, the levels of protection required when handling official documents.

The term document refers to all material assets, ie papers, drawings, images, disks and all forms of electronic data records. This leaflet is designed as an **aid** only.

Further and more comprehensive guidance can be found in the Manual of Protective Security or from your own **Information Security Officer**.

Vetting Levels

The level of vetting will dictate what protectively marked material can be accessed / handled.

A Basic Check (BC) (Baseline Standard) will allow access to protectively marked information up to CONFIDENTIAL and occasional access to SECRET.

A Security Clearance (SC) (Security Check) is required for individuals who are to be employed in posts where they will have long term, frequent and uncontrolled access to SECRET assets and occasional supervised access to TOP SECRET assets.

A Developed Vetting (DV) clearance is required for those individuals who are to be employed in posts where they will have long term, frequent and uncontrolled access to TOP SECRET assets and includes those while not in such posts that are in a position to directly or indirectly bring about the same degree of damage.

For more detailed information regarding vetting contact your own Vetting Officer.