



<b>POLICY</b>	<b>Issue: 4.0</b>
<b>Information Security Policy</b>	<b>Date: 16/12/2010</b>

## 1. Policy Statement

- 1.1 The Civil Nuclear Police Authority (the Authority) and the Civil Nuclear Constabulary (the Constabulary) recognises the need to ensure adequate security for its areas of responsibility and facilities and are committed to managing information and information assets to:-
- a. maintain appropriate security standards, specifically to comply with the; HMG Security Policy Framework, the Office for Civil Nuclear Security (OCNS) Security Policy Framework, Nuclear Industries Security Regulations (NSIR) 2003; Data Protection Act (DPA); 1998 and Freedom of Information Act 2000;
  - b. achieve future compliance of the ACPO/ACPOS Information Systems Community Security Policy (CSP). Through compliance of the CSP and aforementioned standards additionally measure our position against BS (ISO)/IEC 27001: 2005, the Standard for an Information Security Management System;
  - c. ensure the security of protectively marked information and information assets, including those in electronic form, both belonging to the organisation and entrusted to it in accordance with instructions issued to the civil nuclear industry;
  - d. provide security awareness training for all Police Officers, Police Staff and Contractors, including induction briefings, to ensure the integrity of Authority and Constabulary information and assets; and
  - e. ensure, through education and monitoring, that all Users are aware of their responsibility for the security of the data they are processing or accessing and their duty to comply with the 'Information Security Policy' and subsidiary procedures.

## 2. Aims of the Policy

- 2.1 To provide employees and interested parties with clear and concise policy guidance to demonstrate management commitment and support for information security.

<b>Document Reference</b>	<b>CNC/POL/2.3.4</b>	<b>Page 1 of 3</b>
Uncontrolled when printed unless subject to controlled issue Refer to Index of Policies for current version <b>NOT PROTECTIVELY MARKED</b>		

2.2 To ensure the Confidentiality, Integrity and Availability of Authority and Constabulary information in the support of operational and administrative work:

- Confidentiality: Ensuring that the information is not disclosed to unauthorised persons.
- Integrity: Ensuring that the information is accurate and is maintained in its original form.
- Availability: Ensuring information is available when and where required.

2.3 To promote compliance with Government & Regulatory Security Policies and recognised standards for good practice to manage the security of information and information assets within the Authority and Constabulary and the security of information we obtain from access to the IT infrastructures of the policing, criminal justice and nuclear communities.

2.4 Information Security is crucial to ensure that adequate levels of protection are achieved among partner agencies for information sharing projects. The Authority and Constabulary recognises that managing information properly, including the supporting processes, systems and networks, is essential to the intelligence community, the wider police service and partner organisations including the Civil Nuclear Industry, the Crown Prosecution Service and Local Authorities.

### 3. Introduction

3.1 The police service and other organisations in general are faced with increasing security threats from a wide range of sources. These threats include:- espionage; sabotage; computer-assisted fraud; more common threats of wilful and accidental damage; unlawful or unauthorised disclosure of data; human error; carelessness and ignorance. Such threats can lead to failure of core information systems, harm to individuals and breach of criminal or civil law. It is therefore necessary for the Authority and Constabulary to ensure that we protect from misuse and abuse:

- our information systems and information in whatever form;
- any information entrusted to us by others; and
- any information system/s owned by others, such as those of our partners within the policing; criminal justice and nuclear communities.

3.2 We are committed to achieving compliance with the legislation highlighted within the policy statement. These legislation standards form a framework of information security best practice that enables the Authority & Constabulary to achieve a defence in-depth security strategy that encompasses four main areas:

- a Policy and Procedures.
- b Physical Security.

<b>Document Reference</b>	<b>CNC/POL/2.3.4</b>	<b>Page 2 of 3</b>
Uncontrolled when printed unless subject to controlled issue Refer to Index of Policies for current version NOT PROTECTIVELY MARKED		

- c. Personnel Security.
  - d. Technical Security.
- 3.3 This Information Security Policy will apply to all our employees, contractors, professional partners and employees of other companies who are either on our premises or are working remotely. The roles and responsibilities for Information Security are set out within the Authority 'Information Governance Statement'.
- 3.4 'Information' is to be interpreted as being data, which is held either manually or electronically. When the term 'information system' is used, it should be regarded as being the means by which the information is accessed or processed and also applies to manual or electronically held data. The supporting procedures and instructions define how the requirements are to be implemented.
- 3.5 Compliance with the requirements contained within the procedures and instructions represents the minimum required to protect the security of sensitive police information. We have a legal and moral duty to protect and secure the information we hold, in both manual and electronic form, and responsibility for the effective operation of computerised systems, securing the hardware, the software and the network that stores and distributes our information.
- 3.6 This document will be reviewed every two years or when required through Operational necessity.

This policy is enacted by the following management system document references:

<b>Information Security &amp; IT Procedures</b>	<b>Document Ref</b>
The Principles & Means of Security Risk Management	CNC/PP/0420
The Principles & Preparation of Protectively Marked Material	CNC/PP/0654
The Creation, Control & Dissemination of Protectively Marked Assets	CNC/PP/0655
The Copying and Custody of Protectively Marked Assets	CNC/PP/0656
Destruction and Retention of Protectively Marked Assets	CNC/PP/0657
Home and Remote Working.	CNC/PP/0658
Reporting Breaches of Security and Security Incidents	CNC/PP/0415
The Use of Removable Media/Memory Sticks	CNC/PP/0488
Use of Internet	CNC/PP/0449
Use of Corporate Email Systems	CNC/PP/0428

<b>Document Reference</b>	<b>CNC/POL/2.3.4</b>	<b>Page 3 of 3</b>
Uncontrolled when printed unless subject to controlled issue Refer to Index of Policies for current version NOT PROTECTIVELY MARKED		