



POLICY	Issue: 3.0
Security Policy	Date: 01/10/2010

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 all areas of responsibility and facilities within our organisation and are committed to:

- The protection of nuclear material and other radioactive material in process, storage and transit in accordance with the Nuclear Industries Security Regulations 2003 (NISR 2003) issued under the Anti-Terrorism, Crime and Security Act 2001.
- The maintenance of security standards, specifically to comply with the NISR 2003 and the mandatory requirements within the HMG & Office for Civil Nuclear (OCNS) Security Policy Frameworks.
- The upholding of high standards of security as an essential objective.
- The maintenance of effective counter-terrorist protective security measures, including associated training and exercises.
- The application of appropriate security vetting standards for police officers, police staff and contractors employed by or operating within the Authority and Constabulary. The degree of access to nuclear materials or protectively marked information will determine the level of vetting required.
- The security of protectively marked information and assets, including those in IT form, both belonging to the organisation and entrusted to it, in accordance with instructions issued to the Civil Nuclear Industry.
- The provision of security training for all police officers, police staff and contractors, including induction briefings, to ensure the integrity of our information and assets.

2. Aims of the Policy

2.1 The aim of this policy is to set the framework for 'Personnel', 'Physical' and 'Information' aspects of security, each aspect to have its own specific security policy to further outline our aspirations and methodology, to ensure the security of our organisation and personnel and therefore contribute to that of the Civil Nuclear Industry.

Document Reference	CNC/POL/2.3	Page 1 of 3
Uncontrolled when printed unless subject to controlled issue Refer to Index of Policies for current version NOT PROTECTIVELY MARKED		

3. Responsibilities

- Responsibility for security within the organisation rests with the Chief Constable; day to day oversight of security is delegated to the 'Security Manager (SyM)'.
- The SyM is responsible, through the Head of Professional Standards to the Chief Constable, for the development and promulgation of the Security Policies and for providing assurance that the relevant security standards, manuals, procedures and instructions are applied effectively and consistently throughout the organisation.
- Departmental Heads, Unit Commanders and Line Managers, employed by the Authority, are responsible for applying security standards, manuals, procedures and instructions within their areas of responsibility.
- Employees and contractors, working within the organisation have a responsibility for ensuring that they understand and comply with security policies, manuals, procedures and instructions. In addition they have a responsibility for ensuring that they understand and comply with site-specific security policies, procedures and instructions.

4. COMPLIANCE WITH LEGAL REQUIREMENTS

4.1 Application of our security policies will take account of legal and regulatory requirements. All breaches of such policies or the legislation below are considered serious. A breach may constitute a criminal offence for which the organisation will take action. Action may also be taken in respect of any breach using the 'CNC/PP/0413 Disciplinary Procedure' for police staff and the 'Police Conduct Regulations' for police officers.

Data Protection Act 1998 (DPA)

Protects against the illegal disclosure and misuse of personal data. Any breach of the DPA by an individual leads to personal liability under the act.

Copyright Designs and Patents Act 1988

This includes protection against the unlicensed copying or use of software products.

Regulation of Investigatory Powers Act 2000

Creates the offence of intercepting communications on public and private networks unless certain specific conditions are met in which employers may lawfully access employees' communications.

Police and Criminal Evidence Act 1984

Defines conditions under which law enforcement may obtain and use evidence.

Anti-Terrorism and Security Act 2001, Sect 79

Outlines the criminal offence of disclosing information that could prejudice nuclear security. The provisions are intended to deter anyone contemplating making such disclosures and allow those doing so to be prosecuted.

Document Reference	CNC/POL/2.3	Page 2 of 3
Uncontrolled when printed unless subject to controlled issue Refer to Index of Policies for current version NOT PROTECTIVELY MARKED		

Human Rights Act 1998

The purpose of providing policy is to give an indication to staff of the expected course of action. However, it is not possible to cater for every possible combination of factors that would justify a departure from the stated policy. The Human Rights Act 1998 requires the proper use of discretion at all times and nothing within this policy and associated procedural instructions prohibits the use of discretion in appropriate circumstances. Where action is taken that has the potential to interfere with an individuals human rights, the reasons behind the making of the decision should be recorded. Such actions should be necessary, reasonable and justified in the circumstances.

Freedom of Information Act 2000.

Exemptions do not apply to this statement of agreed policy under the Freedom of Information Act 2000.

This policy is further and more specifically detailed by the following policy documents:

Document Reference CNC/POL/2.3.2 Personnel Security Policy;
CNC/POL/2.3.3 Physical Security Policy;
CNC/POL/2.3.4 Information Security Policy.

Document Reference	CNC/POL/2.3	Page 3 of 3
Uncontrolled when printed unless subject to controlled issue Refer to Index of Policies for current version NOT PROTECTIVELY MARKED		