



<b>POLICY</b>	<b>Issue: 2.0</b>
<b>Physical Security Policy</b>	<b>Date: 01/10/2010</b>

## 1. Policy Statement

1.1 Physical security is an essential part of a security plan. It forms the basis for all other security efforts, including personnel and information security. A balanced security programme must include a solid physical security foundation. A solid physical security foundation protects and preserves information, physical assets and human assets. The threats to these assets are:- theft; espionage; sabotage; terrorism; vandalism; natural disaster; catastrophes caused by human failure; accidental damage and other non traditional threats. It requires appropriate layering of physical and technical security such as:- solid building construction; suitable emergency preparedness; reliable power supplies; adequate climate control; CCTV; alarm systems; strong passwords and firewalls.

## 2. Aims of the Policy

2.1 The Civil Nuclear Police Authority (the Authority) and the Civil Nuclear Constabulary (the Constabulary) aims are to set out a physical security framework for our organisation which will, by taking a layered approach to physical security, provide suitably secure environments from which we can operate to achieve our mission.

## 3. Definition of Physical Security.

3.1 In general terms, physical security means the positioning of physical and procedural obstacles to prevent:

- a. Unauthorised access to sensitive material.
- b. Unauthorised access to property for the purpose of destroying, disabling, compromising or removing it, with the object of impeding operations or with the intent of conducting espionage or for financial/personal gain.
- c. Unauthorised access for the purpose of either: - damaging or destroying buildings or facilities used by the Authority or Constabulary, or injuring or killing personnel working therein.

## 4. Guiding Principles

4.1 In particular this policy aims to ensure the Authority and Constabulary will adopt a layered approach to security and will:

- a. Secure the perimeters of our buildings, including all property not owned by ourselves but rented or otherwise provided, taking all reasonable measures to prevent unauthorised access.

<b>Document Reference</b>	<b>CNC/POL/2.3.3</b>	<b>Page 1 of 2</b>
Uncontrolled when printed unless subject to controlled issue Refer to Index of Policies for current version <b>NOT PROTECTIVELY MARKED</b>		

NOT PROTECTIVELY MARKED

- b. Limit building access to our police officers, police staff, contractors and visitors in possession of a valid identity card of our own issue or a relevant site security pass.
- c. Further limit within our buildings, by physical means, access to areas and/or assets where a restricted level of access is either required or deemed as necessary.
- d. Ensure risk assessments are conducted in order to make certain that personnel hold the appropriate level of security to sensitive/high value assets or areas.

Over grading/protection could lead to authorised persons being refused access to the materials/areas they need in order to carry out their duties. Under grading/protection could lead to unauthorised persons being granted access to sensitive material/areas that they have no need to access.

- e. Where the degree of physical security practicably possible will not prevent all possible potential breaches, or in the event of failure of a physical security measure, to have in place appropriate levels of detection systems either physical; technical or both.
- f. Ensure fitness for purpose, uniformity of standards and remain cost effective.
- g. Work with partners to consider security in the design stage of new projects within or for our organisation to ensure our cost effectiveness. Significant security advantages can be derived from the proper positioning of restricted areas and assets within our buildings, as there are also with the positioning of:- buildings; roads; car parks; other services and facilities within a site.
- h. Regularly review the physical security standards within our establishment and be responsive to changes in the threat and environment.

4.2 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>Physical Security Procedures</b>	<b>Document Ref</b>
The Principles & Means of Security Risk Management	CNC/PP/0420
Physical Security: General Principles & Responsibilities	CNC/PP/0414
Reporting Breaches of Security & Security Incidents	CNC/PP/0415
Use of Warrant Cards & Site Passes	CNC/PP/0416

<b>Document Reference</b>	<b>CNC/POL/2.3.3</b>	<b>Page 2 of 2</b>
Uncontrolled when printed unless subject to controlled issue Refer to Index of Policies for current version NOT PROTECTIVELY MARKED		