Physical Security Procedure

This procedure is part of North Yorkshire Police policy to which all Chief Constable personnel and the functions provided by the Police, Fire and Crime Commissioner are required to adhere.

Procedure Statement

This procedure is designed to outline the physical security requirements for North Yorkshire Police (NYP) in order to protect the organisations assets to the required standard.

The objective of this procedure is to prevent any unauthorised physical access, damage and interference to NYP's premises, information and assets.

Physical security involves the appropriate layout and design of facilities, combined with suitable security measures, to prevent any unauthorised access and the protection of NYP, it's people, information, materials and infrastructure.

This requires putting into place, or building into the design, measures that prevent, deter, delay and detect, attempted or actual unauthorised access, acts of damage and/or violence, and that trigger an appropriate response.

The required physical security controls will depend on different factors such as the nature of the threat, the cost effectiveness of the controls, the site and its surrounding environment, whether it is sole or shared occupancy and public access.

The physical security controls may, therefore, be different for each location and it is important that the correct type and mix are implemented.

NYP will adopt a 'layered' approach (Defence in Depth) to physical security.

Overarching Policies:
Information Security Policy

Procedures:
Working with Portable Technology and Documents Procedure
Clear Desk/Clear Screen Procedure
Protective Marking Procedure

Security Incident Handling procedure
Security Incident Reporting procedure

Other Documents:
Code of Practice on the Management of Police Information and Guidance
Information Assurance Governance Strategy
ACPO Community Security Policy
Secure Communications Guidance

Process

The baseline physical security requirements of any location are derived by the sensitivity of the information assets protected within.

This procedure is intended as a general guide to physical security, it does not provide a specific guide for all eventualities. If further information is required please contact the Information Security Officer (ISO) informationsecurity@northyorkshire.police.uk.

The following measures are all mandatory items within the Security Policy Framework, which NYP is mandated to follow:

Defence in Depth

NYP will adopt a 'layered' approach (Defence in Depth) to physical security.

Physical security involves a number of distinct security measures which form part of a 'layered' or 'defence in depth' approach to security. This takes into account the balance between prevention, protection and response. Physical security measures, or products such as locks and doors, are categorised according to level of protection offered.

The 'layered' approach to physical security starts with the protection of the asset at source (e.g. creation, access and storage), this precedes progressively outwards to include the building, estate and perimeter of the establishment. Approach routes, parking areas, adjacent buildings and utilities/services beyond the perimeter are also considered.

The more sensitive the asset, the more barriers (physical or logical) should be placed between it and any potential attacker.

When determining appropriate baseline physical security controls the following factors will be considered:

- the impact of the loss of the site or the asset;
- the threat level;
- the vulnerability of the site or asset;
- the GSC protective marking and associated handling conditions;
- the value of the asset;
- the establishment, including considerations to environment, location and occupancy.

Storage of Sensitive Assets

Critical, sensitive and/or protectively marked assets should be housed in secure areas, protected by a defined security perimeter, with appropriate security and entry controls. The protection provided should be commensurate with the identified risks.

Security Containers

Critical, sensitive and/or protectively marked assets must be secured in appropriate secure containers. Large amounts of critical, sensitive and/or protectively marked material or equipment which cannot be stored in a security container must be stored in a secure room.

Secure Rooms/Secure Areas

A secure area may be a locked office or several rooms within a physical security perimeter. This may be locked and may contain lockable drawers, cabinets or safes. The selection and design of a secure area should take into account the possibility of damage of fire, flood, explosion, civil unrest and other forms of natural or man made disaster. Account must also be made in relation to the relevant Health and Safety regulations and standards. Additional consideration should be given to security threats presented by neighbouring premises.

The following controls are mandatory as per the Security Policy Framework:

- access between public and information processing areas of force premises should be minimised and controlled;
- public areas should contain no signage indicating either the presence or location of areas in which force information is stored or processed;
- shared support functions and equipment (i.e. photocopiers and fax machines) should be sited outside the secure area in order to avoid demands for access that may compromise sensitive information. Secure areas should have their own equipment;
- doors and windows should be locked when areas are unattended;
- external protection should be considered for windows, particularly those with easy external access such as ground floor windows and those adjacent to flat roofs;
- suitable intrusion detection systems, installed to a professional standard and regularly tested, should be used to protect those force premises that hold or provide access to sensitive information;
- hazardous or combustible materials should be stored securely at a safe distance from any secure area. Bulk supplies, such as stationery, should not be stored within a secure area;
- fallback equipment and back up media should be sited in a suitable location in order to prevent it from sustaining damage from any disaster occurring in the main site;
- rooms holding critical, sensitive and/or protectively marked assets must have windows, doors, locks and entry control which meets the appropriate standard;

- the Clear Desk and Clear Screen procedure will be adhered to, screens are not to be positioned where they could be illicitly viewed (i.e. overlooked by a window or reflective surfaces). If this is not possible, other measures must be used (i.e. window blinds). The same principle should apply to other office areas where information is displayed (i.e. wall, white boards etc).

Working in Secure Areas

Additional controls and guidelines are required to enhance the security of a secure area. This includes controls for the personnel and third parties working in the secure area, as well as third party activities taking place there.

The following controls are required:

- personnel should only be aware of the existence of, or activities within, a secure area on a need to know basis;
- unsupervised working within a secure area should be minimised, both for safety reasons, and to prevent opportunities for malicious activities;
- vacant secure areas should be physically locked and periodically checked;
- third party support service personnel should be granted restricted access to secure areas or sensitive information processing facilities only when necessary;
- consideration should be given to additional barriers and perimeters between areas of different security requirements inside the security perimeter;
- photographic, video, audio or other recording should not be allowed unless authorised. Where authorisation has been obtained, use of such equipment should be strictly controlled.

Buildings

In any building in which protectively marked or other valuable assets are stored there should be as few points of exit and entry as possible (allowing for the functions of the building and safety).

Physical protection can be achieved by creating several physical barriers around premises and offices. Each barrier establishes a security perimeter and increases the total protection provided. The position, strength and number of barriers should be proportionate to the assets to be protected and as determined by a risk assessment. Perimeters will typically consist of various elements such as walls or hedges, doors, swipe card or key controlled entry points and manned reception desks.

Open spaces between a security perimeter, and the building it surrounds, should be designed to help patrolling or surveillance, hinder overlooking and deprive any intruder of cover. Where possible, a perimeter should not contain shrubs, bushes or anything offering any intruder cover. Foliage and tall trees should be kept well clear of the ground and fences and shadows they may cast should be taken into account.

The following guidelines and controls should be considered and implemented where appropriate:

- the security perimeter be clearly defined (this applied to sites, buildings, office areas, secure rooms etc);
- the perimeter of sites and buildings containing information should be physically sound (i.e. there should be no gaps in the perimeter or areas where a break-in could easily occur);

- all external walls should be of solid construction;
- windows and external doors should be structurally resistant to forced access and protected by control mechanisms such as bars, alarms and locks;
- a manned reception area or other means to control the physical access to the site or building should be in place;
- external building access codes should be changed every 6 months, as a minimum;
- access to sites and buildings should be restricted to authorised personnel only. Access restrictions should be indicated by clearly worded and prominently displayed signs. However, signs should NOT identify the presence of sensitive information;
- physical barriers should, where relevant, extend from real floor to real ceiling in order to prevent unauthorised entry and environmental contamination such as that caused by fire and flooding;
- all fire doors on a security perimeter should be alarmed and slam shut.

Physical Entry Controls

The following controls are mandatory as per the Security Policy Framework:

- secure areas should be protected by appropriate entry controls to ensure that only authorised personnel are allowed access;
- any visitor to a non-public building must, on arrival, be issued with a visitor's pass and the following details have been recorded:
    - Name
    - Vehicle Registration number (if applicable)
    - Name of the organisation they represent
    - Name of the person they are visiting
    - Time and date of arrival and departure;

- it is the responsibility of the force employee who is being visited to ensure that their visitor is supervised at all times during their visit;
- on departure, the force employee must ensure the visitor's pass is withdrawn and the time and date of departure is recorded;
- where a site or building has a manned reception area, both arrival and departure of all visitors must be made via the reception area;
- access to sensitive information and offices must be controlled and restricted to authorised personnel only;
- all force personnel, contractors and visitors are required to wear their identity passes when on NYP premises;
- it is the responsibility of all staff to challenge any individual that they encounter on force premises who is not wearing visible identification. Any individual who, on being challenged, is unable to produce a force identity card or visitor's pass should either be escorted to the reception area or remain accompanied while enquiries are made into the legitimacy of their presence on force premises;
- when an officer or member of staff (including volunteers) leaves force employment it is the responsibility of the line manager to ensure the identity card and any force keys in their

possession are returned, in addition to ensuring that swipe card access to force premises and password access to force computers has been cancelled and HR Department are informed;

- access rights to secure areas should be regularly reviewed and updated but especially when staff members move or leave.

Isolated Delivery and Loading Areas

Delivery and loading areas should be controlled and, if possible, isolated from office, information processing facilities and storage facilities containing protectively marked material in order to avoid unauthorised access.

The following controls should be in place:

- access to holding areas from outside a force building should be restricted to identified and authorised personnel;
- the holding area should, if possible, be designed so that supplies can be unloaded without delivery staff gaining access to other parts of the building. Where this is not possible, the delivery should be supervised to prevent any unauthorised access by delivery personnel or other individuals;
- the external door (s) of a holding area should be secured or guarded when the internal door is open;
- incoming material should be inspected for potential hazards before it is moved from the holding area to the point of use;
- incoming material should be registered, if appropriate, upon entry to the site.

Equipment Security

The protection of equipment, including mobile equipment and that used off site, is necessary in order to reduce the risk of unauthorised access to data and to guard against loss or damage.

For further information please refer to the Working with Portable Technology and Documents Procedure and the Information Security Policy.

Equipment Position and Protection

Equipment should be sited or protected to reduce the risks from environmental threats and hazards and opportunities for unauthorised access.

The following controls should be in place:

- output equipment, such as monitors and printers, should be positioned to reduce the risk of sensitive information being viewed or obtained by unauthorised personnel;
- measures should be in place to minimise the risk of potential threats, for example:
    - Theft
    - Fire
    - Explosives
    - Smoke

    - Water (or water supply failure)
    - Dust
    - Vibration
    - Chemical effects
    - Electrical supply interruption
    - Electromagnetic radiation;
- there should be no consumption of food or drink in the vicinity of major processing equipment (i.e. servers, hubs and routers). Sensible precautions should be taken to avoid the spillage of food or drink on other equipment;
- environmental conditions should be monitored for elements that might adversely affect the operation of information processing facilities;
- the potential impact of disaster happening in nearby premises should be considered.

Power Supplies

Equipment should be protected from power failures and other electrical anomalies. The electrical supply to all force equipment should conform to the equipment manufacturers' specifications.

The force network is provided with an uninterruptible power supply (UPS). Where practicable, other force equipment providing critical force operations should also be supported by a UPS in order to support orderly close down or continuous running. UPS equipment should be regularly checked to ensure that it has adequate capacity and tested in accordance with the manufacturer's recommendations.

Lightning protection should be applied to all buildings and lightning protection filters should be fitted to all external communications lines.

Cabling Security

Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.

The following controls are required:

- power and telecommunications lines into information processing facilities should be underground, where possible, or provided with alternative protection;
- network cabling should be protected from unauthorised interception or damage by measures such as conduit or by avoiding routes through public areas;
- power cables should be segregated from communications cables to prevent interference.

For sensitive or critical systems, further controls may include:

- armoured conduit and locked rooms or boxes at inspection and termination points;
- use of alternative routings or transmission media;
- use of fibre optic cabling;

- sweeps for unauthorised devices being attached to cables.

Equipment Maintenance

All force equipment should be correctly maintained to ensure its continued availability and integrity.

The following controls are mandatory:

- equipment should be maintained in accordance with the supplier's recommended service intervals and specifications;
- maintenance should only be carried out by ICT staff or by authorised third party contractors;
- a record of all suspected or actual faults affecting the force network and the telecommunications system is maintained by ICT Service Desk. The system owner of any non-networked system should ensure that a record is kept of all suspected or actual faults and subsequent remedial action relating to the system;
- wherever practicable, force equipment, particularly that containing stored data should be repaired or maintained on force premises. Appropriate controls should be implemented where it is necessary to send equipment off premises for maintenance.

Security of Equipment Off-Premises

The use of force equipment away from force premises should be authorised by the relevant Head of Function. The security provided should be equivalent to on-site equipment used for the same purposes but should take into account the additional risks of working away from force premises.

Items involved include all forms of personal computers, radio equipment, mobile phones and paper documents.

The following controls are mandatory and are in addition to any specific operating procedures for particular items of equipment:

- portable equipment or documents should not be left unattended in public places or in unlocked vehicles. Any hand held portable equipment or documents left in a vehicle must not be visible from the outside of the vehicle. Please note that a locked vehicle does not constitute a secure environment;
- laptop computers should be carried as hand luggage and disguised where possible when travelling;
- manufacturers' instructions for protecting equipment should be observed at all times (e.g. protection against exposure to strong electromagnetic fields);
- home working controls should be determined by a risk assessment and suitable controls applied as appropriate (e.g. lockable cabinets, clear desk, clear screen and access controls for computers). Force information should never be placed on a force employee's privately owned computer.

Secure Disposal or Re-use of Equipment

Information can be compromised through careless disposal or re-use of equipment. All items of unwanted, damaged or obsolete equipment with storage devices (e.g. hard disks) that contain protectively marked or other sensitive information should have the storage devices removed and retained by ICT prior to any disposal of equipment. The storage devices should either be fully overwritten or be physically destroyed.

All disposal or re-use of equipment must be in accordance with the appropriate national standards.

General controls

Adequate controls need to be in place in order to protect information and information processing facilities from theft and unauthorised disclosure or modification.

Responsibilities

All Officers and Staff

Are to be familiar with the Physical Security Procedure and should act accordingly to protect the security of NYP information, materials, and premises.

First Line Supervision

Are to ensure their staff are aware of, and adhere to, the Physical Security Procedure. In addition, supervisors must report any incidents arising from the

non-adherence to this procedure.

Heads of Functions/Safer Neighbourhood Commanders

To ensure the continuing physical security of NYP information, premises and materials and that any breaches of security are recorded and managed in an effective risk based manner.

Orderly and Secretarial Account Lead / Property and Facilities Management

To ensure properties within their remit have all external door codes changed every 6 months as a minimum and have in place a mechanism for recording and communicating scheduled changes.

Chief Officer Team

Overall responsibility for the physical security of all NYP information, premises, materials and assets.

Definition of Special Terms

GSC	Government Security Classifications
ISO	Information Security Officer
CTSA	Counter Terrorism Security Advisor

UPS	Uninterruptible Power Supply
ICT	Information Communications Technology