Physical Security Policy Template

The Free iQ Physical Security Policy Generic Template has been designed as a pre-formatted framework to enable your Practice to produce a Policy that is specific to your requirements.

The Policy ensures that you review all physical security issues relating to the Practice in preparation for any Service Continuity Planning.

INSERT NAME & ADDRESS OF PRACTICE	***Insert Practice Logo***

Physical Security Policy

Insert Date

TABLE OF CONTENTS PAGE No.

STATEMENT

The security and protection of practice assets, facilities, personnel and patients is fundamental to the effective and efficient working of the practice.

This Policy provides a framework which allows us to manage resources in the most secure way.

Security is everyone's responsibility and all personnel working in the practice must make every effort to comply with this Policy.

SCOPE OF POLICY

THE NEED

To meet legal and professional requirements the practice must use cost effective security measures to safeguard its physical resources.

This Physical Security Policy will ensure a consistent approach to the implementation of appropriate security controls against common threats.

THE POLICY

The Policy of the practice is to accept willingly all obligations in respect of physical security and to protect its resources by implementing recognised best practices that will achieve a balance between cost and risk.

APPLICABILITY

The Policy shall apply to all partners and staff of the practice and any other healthcare professional using the resources of the practice.

IMPLEMENTATION

- The requirements of the Policy shall be implemented by all partners, staff and other healthcare professionals using the practice's resources.
- Any team member noting any area of conflict between this Policy and any other practice Policy must bring it to the attention of the ***Insert Name and Position of Person*** as Security Officer of the practice, immediately for conflict resolution.

  The ***Insert Name and Position of Person*** will in any case be responsible for the routine periodic review of the Policy.
- Internal audit shall undertake independent reviews to assess the adequacy of implemented security measures including compliance with the Policy.
- Compliance with the Policy is the duty of all partners and staff.

  In serious cases, failure to comply with the Policy may be a disciplinary matter and could also result in a breach of the law or a criminal offence.
- Staff have an obligation to report suspected breaches of the Policy immediately to the Practice Manager.

INFORMATION RESOURCES

The Policy applies to any resource, which is owned, held in the custody of, or used by the practice.

OBJECTIVES OF THE POLICY

The objectives of the Policy are to ensure that:

- Resources are protected from accidental or malicious damage.
- Security risks are properly identified, assessed, recorded and managed.
- Safeguards to reduce risks are implemented at an acceptable cost.
- All legal, regulatory and contractual requirements and standards of due care are met.

These objectives shall be achieved through the implementation of security controls as described in the remaining sections of this Policy.

LEGAL OBLIGATIONS

GENERAL

The practice accepts its obligations to comply with the laws of the United Kingdom.

KEY SECURITY CONTROLS

GENERAL

- The ***Insert Name and Position of Person*** and ***Insert Name and Position of Person*** will ensure that all contracts of employment and any contracts of agency staff include a security compliance clause.
- The ***Insert Name and Position of Person*** and ***Insert Name and Position of Person*** will ensure that security responsibilities are allocated to staff and written into job specification and terms of reference.
- Security education and training will be provided to all staff as appropriate to their assessed needs.

PHYSICAL SECURITY CONTROL

1. Principle

Resources associated within the practice, including office machinery, IT equipment, clinical equipment and the practice building shall be protected from unauthorised access, misuse, damage or theft.

2. Access

- The non-public areas of the practice premises are designated a secure area.

  Visitors are to be escorted at all times and a record of visitors kept in Reception.
- In order to prevent unauthorised access during silent hours an Intruder alarm system is provided.

  Reaction to alarms and subsequent management action are detailed in the practice Health and Safety Policy.

3. Equipment

- All assets held by the practice are to be held against an asset register and be uniquely marked as being the property of the practice.
- All equipment storage areas are 'out of bounds' to visitors.
- On-going maintenance arrangements are to be made for all essential equipment and installations and are to be reviewed at regular intervals by the ***Insert Name and Position of Person***.
- Equipment is not to be removed from the practice without the authority of the ***Insert Name and Position of Person***.

4. Risk Assessment

- The practice is to have a system of Risk Assessment in place to cover all areas of physical security.
- Adequate, cost effective controls are to be implemented to reduce the level of associated risk.

INTERNAL SECURITY CONTROL

1. Access Controls

- The following key personnel are issued with keys to access the main door, front security shutter and side gate, along with the Intruder Alarm Access Code.
  - ***Insert Names and Positions of Persons***
  - ***Insert Names and Positions of Persons***
  - ***Insert Names and Positions of Persons***
  - ***Insert Names and Positions of Persons***
- Individuals are to ensure the safe keeping of the keys to prevent unauthorised access. Any loss of keys is to be reported to the ***Insert Name and Position of Person*** without delay.
- The rear entrance door to the first floor and the clinical store are protected by a keypad security lock.
- Keypad combinations are to be kept confidential at all times.

  Anyone who considers that a combination has been compromised is to notify the ***Insert Name and Position of Person*** without delay.
- Keypad security combinations are to be changed at agreed regular intervals.

2. Security Incidents and Reporting

- At the end of each working day, all room occupants are to ensure that windows are fully closed and secured.
- All electrical equipment, with the exception of essential IT equipment (Server, Fax, Telephone system etc) is to be switched off at the end of each working day.
- At the end of the working day, the Cleaning Team is responsible for:
  - Ensuring that all security shutters are closed.
  - Ensuring that the rear entrance door to the first floor is secured.
  - Ensuring that the Intruder Alarm is set.
  - Ensuring that the main door is secured.
  - Ensuring that the side security gate is secured.

3. Service Continuity Planning

Physical Security is to be incorporated into the practice Service Continuity Plan to ensure the continued fulfilment of the practice mission.

4. Violence & Aggression

- The practice operates a Zero Tolerance Policy toward violence and aggression.
- At some time we may all come in contact with patients who are violent or aggressive.

  The definition of work related violence is not subjective.

  'Violence' means:

  > *'Any incident where staff are abused, threatened or assaulted in circumstances related to their work, involving an explicit or implicit challenge to their safety, well-being or health'.*

- Violent and abusive behaviour also includes such behaviour over the telephone.
- Violence and abuse is **not** part of your job.

  The practice will not tolerate any violent or abusive behaviour toward its staff and will do all it can to ensure the safety of its staff.

  Patients are advised of our Policy regarding violence and a notice is displayed at Reception.

  Violence against staff is a crime and the practice will take whatever action is necessary to prosecute offenders
- The practice Protocol '***Dealing with Violent and Aggressive Events'*** is to be followed at all times.

EXTERNAL SECURITY CONTROL

1. Patient Access

Patients are not to be allowed entry to the practice premises until a minimum of two receptionists are on duty.

2. Security Shutters

All ground floor doors and windows are fitted with security shutters. All shutters are to be fully closed when the building is closed.

The ground floor rear fire door shutter is to be kept raised at all times when personnel are in the building.

3. Outside Areas

The exterior of the building and the practice car park is illuminated by security lights from dusk until dawn. Faults with the external lighting are to be reported to the ***Insert Name and Position of Person*** without delay.

Staff are to be vigilant when walking to and entering their cars, especially during winter and during the hours of darkness. Wherever possible, staff are to leave the building in groups.

SECURITY INCIDENTS AND REPORTING

A security incident is defined as any event that could result or has resulted in:

- The integrity of the working process being put at risk.
- The availability of a resource being put at risk.
- An adverse impact, for example:
  - Embarrassment to the practice, PCT and NHS.
  - Threat to personal safety.
  - Legal obligation or penalty.
  - Financial loss.
  - Disruption of activities.

All incidents or information indicating a suspected or actual breach of security must be reported immediately to the ***Insert Name and Position of Person***. The types of incidents that can result in a breach of security are many and varied.

Their severity will depend upon a myriad of factors but the majority will be innocent and unintentional and will not normally result in any form of disciplinary action. The likely result will be improved security and awareness throughout the practice.

Any unusual incident must be reported to the ***Insert Name and Position of Person*** using the Significant Event Reporting procedure.

Any member of staff reporting a breach of security will have unhindered access to the ***Insert Name and Position of Person***. If that member believes the breach is as a result of an action or negligence on the part of the ***Insert Name and Position of Person*** then the member will have access direct to the ***Insert Name and Position of Person***.

TRAINING

Staff training is to be provided covering the following:

- Physical Security
- Dealing with violence and aggression / Conflict resolution
- Risk Assessment

Training is to be carried out annually and recorded on staff training records. ***Insert Name and Position of Person***is responsible for arranging all training.

ROLE OF THE PRACTICE SECURITY OFFICER

The ***Insert Name and Position of Person*** is the nominated Security Officer for the practice and shall:

- Under the direction of the Partners, develop and manage the practice security programme.
- Develop, issue and maintain the physical security strategy and Policy and agree them with the Partners.
- Develop a strategic Service Continuity Plan and advise the practice on its implementation.
- Create a security awareness programme to include practice briefings, training and education.
- Provide security consulting support to the practice.
- Investigate breaches of security and report findings and recommended action to the practice.
- Implement a compliance programme to evaluate the effectiveness of the physical security programme.
- Report annually to the Partners on the effectiveness of the overall physical security programme.

POLICY REVIEW

This Policy is to be reviewed on an annual basis by the ***Insert Name and Position of Person***to take account of changing circumstances, legislation, technology and security risks.

Any revisions to the Policy are to be approved by the Partners prior to implementation.

LINKS TO OTHER POLICIES

This Policy links with, and is to be read in conjunction with, the following:

- Health and Safety Policy
- Information Security Policy
- Service Continuity Plan

STAFF COMPLIANCE AGREEMENT

All employed and attached staff are to read this Policy and sign a certificate of compliance.

An example certificate is in **Annex A** overleaf

Signed certificates are to be retained by the ***Insert Name and Position of Person***.

ANNEX A – STAFF COMPLIANCE AGREEMENT

INSERT NAME & ADDRESS OF PRACTICE	***Insert Practice Logo***

Physical Security Policy
-
Staff Compliance Agreement

I have read and understand
the Practice Physical Security Policy
and agree to abide by the requirements laid down in the Policy.

Name	
Signature	
Date	

This Agreement is to be signed by all personnel working at
******Insert Name of Practice******
and is to be retained in the register maintained by
******Insert Name and Position of Person******