For information

Legislative Council Panel on Security

Security of Police Stations and Personal Data held by the Force

Purpose

This paper sets out the information requested by Members of the Panel on Security on a number of issues regarding the management and security of Police stations.

Access to databases and records, especially personal data, in a Police Station

2 The Force has formulated policies for data administration (including personal data) which sets out the overall responsibilities and procedures to ensure that all users adhere to defined standards. In relation to data involving personal data, police officers must also comply with the requirements of the Personal Data (Privacy) Ordinance (Cap. 486). The Force has promulgated internal instructions setting out specific procedures regarding the handling of documents containing personal data. Officers are also required to observe the Government Security Regulations and internal instructions on the security of the Force's computer systems (including storage, processing, transmission and management of classified information, data encryption and physical security of computer systems). Violation of the above requirements will result in disciplinary actions, or criminal prosecution in the event of unlawful access to a database.

3. In Police stations, all electronic case data are stored in the Force Communal Information System (CIS) and the following measures are in place to protect the security of such data –

(a) Only dedicated terminals in the Police stations have access to the CIS. Authorised officers' access to the CIS through these terminals is controlled by password, which has to be changed every three months. The designated System Security Manager (normally of Chief Inspector or Superintendent rank) strictly controls the issue/revocation of passwords in each station.

(b) The degree of access that a police officer has to information stored in the CIS is determined by reference to the relevance to his role in the case, his post and/or seniority. An investigator can access

only those cases and data within his own responsibilities.

(c) For control and audit, the system automatically records each access to the CIS by individual officers. Supervisors can check access made to CIS records of cases under their responsibilities.

As regards case data recorded in paper files, in a similar vein, an investigator can only access those files on cases assigned to him for investigation.

4. PGO 53-01(6) requires police officers to record information relating to their constabulary duties in their official police notebooks. PGO 53-01(3) further provides that an officer shall ensure that he complies with Data Protection Principle Four of the Personal Data (Privacy) Ordinance[1] and that the personal data entered into his notebook is to be strictly limited to that which is necessary to enable him to effectively discharge his constabulary duties; and is recorded in such manner that it cannot be subsequently read by any non-authorised person. Accordingly, it is not necessary to keep record of every detail of the personal particulars of a person after the exercise of any police power. In most cases, basic information that is sufficient to identify the persons concerned would suffice.

5. The PGO requires that all documents created by the Force and containing personal data shall be so classified or marked insofar as it is reasonably practicable to do so. An officer may take such documents with them when off duty only with the written permission of his supervisor.

Security of Police Stations

(a) General Security Requirements

6. Furthermore, Formation Commanders issue standing orders on station security for compliance by all police officers in each station. These standing orders reflect the following principles enshrined in the Government Security Regulations regulating security in government/joint-user premises –

(a) heads of departments are responsible for building security;

(b) buildings must be secured after office hours and rooms checked by occupants prior to leaving;

---

[1] Under Data Protection Principle Four of the Personal Data (Privacy) Ordinance (on security of personal data), all practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure or other use.

(c) keys to locks used for the protection of classified material must be safeguarded at all times, with officers concerned being personally responsible for their safe custody;

(d) control of entry is best exercised by use of one specified entrance; and

(e) visitors to secure areas should be escorted at all times.

7. Formation Commanders' standing orders lay down detailed requirements regarding access to rooms other than communal areas which are used round the clock.

8. Access to these other areas is subject to control as illustrated below –

(a) Cell and detention facilities: Report room staff inspect these facilities regularly. Access is strictly controlled by the Duty Officer and the entrance to those facilities is usually covered by CCTV;

(b) Armouries: Only designated officers who are properly trained have access. Supervisory officers who inspect these facilities regularly are also authorised access;

(c) Floors with restricted areas: These areas are fitted with digital locks and access is code-controlled. The code, which is changed regularly, is provided only to those officers with a need to access these areas; and

(d) Rooms which contain valuable items: These include property offices and rooms with a large number of computer or electrical equipment. Only authorised key-holders may have access to these rooms which are locked when not in use.

9. In general, unoccupied office accommodation is kept locked. Police officers working in a police station are provided with keys to offices/rooms which they work in. Keys for other areas of the station are held in a secure location by either the Duty Officer or Administration Support staff. Officers who need to access these areas have to sign for the keys.

(b) Access to a Police station

10. Vehicular access to station compounds and pedestrian access into Police station buildings via staff entrances are controlled by the Automated

Station Security System. This System, which is used to control access to a Police station, comprises a CCTV system, a building access control system and an automated vehicle access system as follows –

(a) CCTV Monitoring System: Digital images of activities in and around the station are captured by a CCTV monitoring system and stored in a digital video recorder. The number of CCTV cameras and locations covered depend on the circumstances of individual Police stations.

(b) Building Access Control System: A police officer has access only to his or her respective Police station. He must use his Police warrant card to gain access to a station compound through a pedestrian gate and non-public areas of a Police station.

(c) Automated Vehicle Access System: Only those vehicles with an authorized pass can access a station vehicle compound. Such access is granted to a limited number of officers serving in a Police station who have a parking permit for that station. If a vehicle without the afore-mentioned access authorisation requires access to a Police station, the driver has to make a request to the report room.

11. All visitors to a Police station are required to register at the report room on arrival. If after enquiry, the report room staff consider it appropriate to grant access, they will issue a visitor pass to the visitor following verification and recording of his/her identity. Throughout the visitor's stay in the Police station, he/she should be escorted by an officer assigned to handle the visitor.

12. Formation Commanders' standing orders contain detailed guidelines regarding other aspects of station security, e.g. security of barrack accommodation, access to fitness rooms and resource centres, registration and escort of visitors, etc. In addition, the standing orders contain specific instructions for the Duty Officer to conduct regular station checks in order to maintain security, prevent fires and for "green management" purposes. The instructions also include procedures for supervisory checks by officers of Chief Inspector and above ranks outside office hours and during holiday periods.

Conclusion

13. The Force attaches great importance to information security and the security of Police stations. The Force has instructions in place covering station security and has also issued further instructions in respect of information technology security and protection of personal data. Police officers are

required to strictly comply with orders and instructions promulgated within the Force in this regard. Disciplinary actions will be taken against officers who fail to observe these requirements. Since June 2008, the Force has launched a series of awareness campaigns to emphasize the requirements to control access to computer systems and protect personal data. Moreover, "Information Security and Protection of Personal Data" is one of four key Communication Priorities adopted by the Force since September 2008. Key messages on this subject are also cascaded down to the Force through training packages and communication forums.

14. The Force will keep under review the security arrangements for Police stations and personal data held by the Force, and will introduce further improvement measures where necessary. For example, the Force has plans to step up the security requirement by requiring all officers, in the longer term, to use both warrant card and password for access to the CIS. The Police are also considering enhancement of the Automated Station Security System by expanding the use of CCTV and swipe readers to cover more areas of a Police station.

Hong Kong Police Force
January 2009