POLICE GENERAL ORDERS

CHAPTER 19

INFORMATION AND COMMUNICATIONS TECHNOLOGY FACILITIES

18/09

19-04 Provision and Disposal of Computer and Communications Facilities and Equipment

11/16

All Force Information and Communications Technology (ICT) equipment and facilities shall be procured, installed, relocated, repaired, enhanced and disposed by or through arrangements made by the Information Systems Wing (ISW). Relevant procedures and workflows as laid down in the Client Focused Account Management System 3 (CFAMS3) should be followed. The security measures of all Force ICT equipment and facilities shall observe the Government Security Regulations as well as the Force Information Security Strategy (FISS).

19-12 Care of Force ICT Equipment

11/16

ICT equipment inventory holders shall be responsible for the physical storage, security, day-to-day accounting and inspection of equipment under their charge.

2. Formation Commanders shall ensure that:-

(a) all ICT equipment and facility users must conform with the manufacturers' and ITB/COMMS operational instructions, cautionary and safety measures;

(b) only Force members will be allowed to use any ICT equipment and facility for which training is required;

17/14

(c) Force communications equipment not in daily use shall be functionally tested and physically inspected not less than once every quarter or in accordance with the instructions given by the manufacturer or COMMS and the instructions to handle the batteries (if the equipment are battery powered) shall be followed to avoid damage or malfunction; and

(d) aerials, microphone units or accessories shall only be attached to or detached from radios and other Force communications equipment by trained armoury staff or authorised personnel only.

3. Force ICT users are not permitted to tamper with or dismantle any Force ICT equipment or accessories. Only ISW staff or authorised personnel are permitted to do so for the purposes of maintenance or repair.

02/13
11/16

19-14 Reporting of Damage/ Loss of ICT Equipment

An officer who discovers the loss or damage of any ICT equipment, including rental and hired equipment, shall immediately report such loss or damage in accordance with the requirements laid down in PGO/FPM Chapter 14. The Formation handling the loss or damage of the ICT equipment shall ensure relevant provisions of PGO/FPM Chapter 14 are complied with. In case of loss of equipment containing Force data, the provisions of FPM 19 shall also be observed. Reference should also be made to the Incident Response and Management Roadmap on POINT.

2. The ISW Information and Communication Network Management Centre (ICNMC) is responsible for deactivating Force Mobile Radio Telephones (FMRT) service only but not reactivation of the service or replacement of a lost FMRT. Any loss of FMRT shall be reported immediately to ICNMC for service deactivation. If reactivation of service or replacement is required, the user Formation shall raise a request to ISW via the Client Focused Account Management System 3 (CFAMS3) for arrangement. The same process is also applicable to the loss of Force Smart Devices.

3. Upon the conclusion of investigation as per FPM 14-03, Formation Commander is required to forward a copy of the 'Report on Loss of/ Damage to Government Stores' (Pol. 225)
17/14 to ISW (Attn.: SP BSD). In all loss and beyond-repair damage cases, the procedures in FPM 14-05 are to be followed to write-off the ICT equipment, following which a CFAMS request is to be made to seek replacement, if necessary.

4. The loss of ICT storage equipment (e.g. portable computer, data storage devices such as floppy disks, CD/DVDs, PDAs, USB storage devices) containing classified information or personal data is considered a breach of security. The holder must report immediately to his/her
17/14 Formation Information Technology Security Officer (FITSO) who shall report to ACP IS (Attn.: SP S&S BS) within 24 hours. The procedures of FPM 19-22 and 19-23 shall be followed.

5. Loss of Force issued USB thumb drives containing Force data must be treated seriously with high sensitivity. The Formation Commander concerned must conduct a risk assessment in accordance with FPM 19-23. The risk assessment report shall reach ACP IS (Attn: SP S&S BS) within 72 hours from the time of reporting loss.

19-15 General Rules in using ICT Facilities and Equipment

02/13
17/14
11/16

Formation Commanders are required to keep an updated record of all ICT equipment on the Stores Management System (STORESMAN) including holders' information and serial/identification number of respective equipment under his/her Formation charge. All ICT inventory discrepancy should be brought to the attention of ISW (Attn.: SP BSD).

2. Formation Commanders shall ensure that computer and telecommunications equipment rooms, Police telephone equipment room, and 999 facilities including their associated equipment and battery rooms, are locked and out of bounds to all unauthorized personnel. These rooms must not be used as storerooms or other purposes. Formation Commanders shall ensure the access keys to the equipment rooms be kept securely with respective Duty Officer or in a way that could be accessible round-the-clock upon request by ISW technical support team. In addition, Formation Commanders shall arrange regular checks no less than once per month on the environmental condition and the functioning of air-conditioners in these rooms using the Checklist at Annex 'E' in the Force Information Security Manual (FISM) and report any signs of hazards, including water seepage, to the EMSD or ArchSD at once. Formation Commanders shall ensure the completed checklist is properly filed for inspection purposes. The ISW ICNMC (2860 3444) shall be notified immediately when any irregularities are noted.

3. Officers shall be responsible for all chargeable services, including but not limited to IDD calls, roaming, SMS, MMS, mobile data services and other information services, made from or accepted on Force communications equipment including a calling card under their charge. He is liable to refund to the Government the full cost of all such charges not made on approved official business.

4. Messages for dispatch from the Force IDD facsimile terminal at PHQ COMCEN shall be submitted to an officer of Inspectorate rank or equivalent for approval of content and authorization for dispatch before forwarding it to the DO PHQ COMCEN.

5. DO PHQ COMCEN shall ensure that all incoming facsimile and documents are forwarded or transmitted to the appropriate officer for action as soon as possible.

6. The usage of all Force ICT equipment is for official purposes only unless otherwise specified. Officers shall be responsible for the proper care and use of Force ICT equipment, and shall be liable for any charges arising from misuse, damage or loss of such equipment in their custody. Officers shall not permit any person other than ISW staff or authorized contractors to tamper with, or make any attachments or alterations to such equipment under their control.

11/16 **19-16 Issue and Receipt of Portable Radios**

A Beat Equipment Register (Pol. 10A) shall be kept in each armoury for recording every issue/receipt of portable radios. Portable radios and associated ancillary items shall be accorded the same degree of security as for arms and ammunition.

2. The issue of portable radios to a group of personnel (e.g. a duty shift parading for duty) shall be supervised by an officer not below the rank of SGT. The return of radios shall be similarly supervised.

3. An officer, upon being issued with a portable radio, shall sign the Pol. 10A in the armoury and be responsible for the care and safe custody of the equipment until such time as it is returned and signed back into the armoury or properly handed over to another officer.

4. Officers who have been issued with portable radios shall return them to the armoury immediately on completion of their duty, except when the officers are on immediate standby.

5. Armoury duties are to check the radios carefully when they are returned to the armoury to ensure that the radios have not been tampered with.

02/13 6. In cases where radios are reported as being lost or missing, the ICNMC of ISW shall be notified immediately to deactivate the radio functions.

17/14 11/16 **19-21 Information Security**

Information Security relies on the collective effort of every Force member. The Force Information Security Strategy (FISS) has been in placed for compliance of all to protect and prevent Force information from unauthorized or accidental access, use, disclosure, disruption, modification or destruction with a view to ensuring the confidentiality, integrity and availability of the information. The Force Information Security Manual (FISM) contains information, advice and guidelines on information security. While non-compliance of the content of the FISM does not necessarily constitute a breach of an order, recurrent or blatant disregard for FISM renders an officer liable to disciplinary action.

2. To strike a balance between the convenience of ICT and the necessity of information security, every Force member must comply with the following Force information security policies and their specific instructions in FISM:-

(a) **Information Access Policy** – all Force members shall only access information held in an ICT system on a "Need to Know" basis and in connection with their official duties. Privileges to users shall be assigned according to the least privilege principle.

(b) **Physical Security Policy** – sites chosen to accommodate ICT equipment which store or process information or electronic data should be risk avoidance to theft, water and heat damage. Formation Information Technology Security Officer (FITSO) should seek help from EMSD, ASD or the respective personnel of BSD for relocation arrangement where necessary.

(c) **Personnel Security Policy** – security vetting on integrity may be required for personnel who has access to classified or sensitive information or data. Training should be provided to staff who uses ICT equipment to minimise the possibilities of accidental disclosure or erasure of data.

(d) **Hardware and Software Asset Management** – workflow of the Client Focused Account Management System 3 (CFAMS3) should be followed to handle procurement, deployment, relocation and disposal of ICT equipments and facilities. The Stores Management System (STORESMAN) should be updated as soon as practicable to facilitate inventory check (FPM 14-10) and inspection made under FISM. 02/13

(e) **Data Classification Policy** – ICT System Owners or information originator shall accord suitable classification and markings/labels on files/documents, mediums or protective containers of classified audio, visual recordings and data on removable or portable media in accordance with Chapter III of the Government Security Regulations so that appropriate security measures on ICT systems may be applied.

(f) **Data Control Policy:-**

(i) All classified information or data (e.g. personal data) in either electronic or hardcopy form shall be regarded as potentially sensitive and measures shall be taken to guard against loss, unauthorised access or leakage. The security requirements stipulated in the Government Security Regulations shall be complied with.

(ii) ICT System Controller shall implement security measures to prevent unauthorised disclosure of information and data processed or stored by the responsible system. Officers who handle the information or data also have the responsibility to do the same.

(iii) Security measures such as encryption using Force provided tools, and password protection of electronic files/data shall be taken to protect sensitive or classified information. Any information or data of or above 'RESTRICTED' classification including personal data shall be encrypted when stored in Force Smart Devices and removable storage media issued to individual officers.

02/13 (iv) Force members are not permitted to use their private ICT equipment (e.g. mobile devices, personal computers, memory cards, USB thumb drives or non-government provided storage facilities) to store electronic classified information or data. Requirements in FISM shall be followed for the approval and use of private ICT equipment for official purpose.

(v) Force members shall not carry any information or electronic data (stored in any media) of or above 'CONFIDENTIAL' classification off police premises unless prior approval from direct supervisor at SP rank or above has been obtained.

(vi) Classified documents shall not be sent via email, facsimile or the Internet unless such facilities are equipped with encryption facilities approved by ISW. Members are also required to follow the instructions stipulated in PGO/FPM Chapter 76 when handling personal data.

(g) **Network Security Policy** – The Internet is a public platform for worldwide information exchanges. Information transmitted over the Internet is susceptible to interception or accidental disclosure to the public. Officers shall not transmit police information of or above 'RESTRICTED' classification via the Internet or other untrusted domain without encryption in accordance with the Government Security Regulations and FISM.

02/13 (h) **Remote Access Security Policy** – Force members are allowed to access Force ICT systems through official (e.g. POINT from Home, Access from Home) or pre-approved channels (e.g. Force Smart Devices, secure channels for remote maintenance by authorised staff or contractors) only.

(i) **E-mail Security Policy** – The Police E-mail Network (PEN) is provided to Force members for duty purposes. Registration of PEN e-mail address with non-duty related websites should be avoided. PEN is permitted to transmit information among Police Formations and other Government Departments only with mail content up to 'RESTRICTED' level. Alternatively, users are allowed to transmit attachment containing 'CONFIDENTIAL' information within PEN environment, which shall be encrypted by Force provided digital certificates and encryption tools. If both sender and recipient are Confidential Mail System (CMS) or Confidential Messaging Application (CMSG) users within the Government, CMS or CMSG can be used to transmit mail content consisting of 'CONFIDENTIAL' information. Details governing the use of PEN can be found in FPM 19-24. Force members should beware that e-mail services not provided by the Force are generally insecure, and hence transmission of sensitive or classified information should be via Force provided E-mail systems i.e. PEN, CMS, CMSG or other dedicated communication links. 18/14

(j) **Anti-Virus Management Policy** – Force ICT systems and facilities need to be protected by anti-virus software with latest virus definition which are updated automatically. Force members in charge of ICT equipment (e.g. laptop, standalone computers, android-based Force Smart Devices) without automated anti-virus update support shall conduct manual update as per the instruction promulgated by ISW from time to time or seek assistance from the ICNMC should they encounter problems in updating.

(k) **Use of Privately Owned ICT equipment for Official Work Policy:-** 12/18

(i) Force members are not permitted to use their private computers or any form of data storage devices for official duty purposes without prior approval. All special applications shall be referred to ACP IS for approval.

(ii) Force members may however use their private mobile phones for situational awareness purpose provided that no classified data is involved. Using private mobile phone for gathering evidence or capturing personal data purpose is not permitted.

(l) **Clear Desk Policy** – Force members shall ensure that all sensitive or classified information in any form such as documents and data storage media (e.g. floppy disks, CD/DVDs, USB drives, memory cards, etc.) are properly secured from unauthorized access when they are away from their offices or desks.

(m) **Password Security** – It is the responsibility of individual ICT user to maintain the confidentiality of any password issued to him/her for accessing any Force computers, applications, e-Services and Force Smart Devices. No officer is permitted to access a system using another user's username/password or to share his/her own username/password with other users to access the system. Formation Commanders and holders of FMRT or calling card shall ensure that confidential details such as the FMRT or calling card service code numbers and Personal Identity Number (PIN) are not divulged to unauthorized persons.

17/14 **19-25 Security Compliance – Self Assessment and Audit**

The ISW Security Team, as directed by ACP IS, shall perform ICT Systems Security and Compliance Audits on Force ICT systems and user Formations. Formation Commanders and officers shall facilitate the access to all Force ICT equipment, facilities, relevant documentation, work areas, computing suites and data storage areas by ISW Security Team personnel for the purposes of the audit.

02/13 2. Formation Commanders or Systems Owners who wish to be exempted from the audit may apply to ACP IS (Attn: SSP BSB) in writing with full justification.