



CENTRAL POLICE OFFICE,  
PUNJAB, LAHORE.

STANDING ORDER NO. 02/2024

**SUBJECT: DATA PROTECTION OF THE DATA MAINTAINED BY THE POLICE  
COMPUTER/INFORMATION SYSTEMS**

**I- INTRODUCTION AND RATIONALE**

The Punjab Police operates under the Police Order, 2002, Punjab Police Rules, 1934 and statutory Standing Orders issued by the Provincial Police Officer under the law. Under Articles 163 and 166 of the Police Order, 2002 read with Chapters XXI, XXII, XXXIII, XXIV, XXV and XXVI of the Police Rules, 1934, it is authorized to collect, retain, edit, process, store, disseminate, share and remove data in its manual and computerized databases. In order to streamline the system of processing data, this Standing Order shall be adhered to in letter and spirit.

**II- CHIEF DATA OFFICER**

The Deputy Inspector General of Police, Information Technology shall be the principal staff officer of the Inspector General of Police in relation to all data related matters. He shall be the chief data officer, and in this capacity, he shall be the custodian of the data and servers of the data collected, processed, retained, edited, disseminated and shared by the Punjab Police. He will be assisted by all the staff officers of the Inspector General of Police in maintaining the integrity and in ensuring that the data of the police is secured and all protocols with respect to cyber security are integrated into computer/information systems. He shall coordinate with the Punjab Information Technology Board and the Punjab Safe City Authority on behalf of the Inspector General of Police.

### **III- DATA PROTECTION**

1. The data with police shall be fully protected according to the international standards and shall comply with the laws/policies related to cyber security;
2. The integrity of the data shall not be compromised and all the data shall be maintained as per the instructions of the Inspector General of Police;
3. All field officers (Heads of the District Police) shall ensure that instructions issued by the DIG/IT are followed in letter and spirit;
4. The data related to the Crime Record Office (CRO) shall be maintained as per the record of the registered criminal cases and editing, if any, shall be carried out as per this Standing Order or due to any court order;
5. The data related to the CRO shall be entered and processed under the supervision of the Head of the District.

### **IV- DATA RECTIFICATION AND ERASURE**

1. Any matter related to rectification and erasure of the data shall be placed before a Verification Committee, which shall make recommendation to the Inspector General of Police for any rectification and erasure.
2. The Verification Committee shall comprise:
  - a. Capital City Police Officer/Regional Police Officer (Convener)
  - b. City Police Officer/District Police Officer (Member)
  - c. Senior Superintendent of Police, RIB (Member)
  - d. Superintendent of Police, Legal/DSP, Legal (Secretary)
  - e. Incharge CRO of the concerned District (Member)
  - f. Any other coopted member by the Convener
3. The Verification Committee on receipt of an application or court order related to data shall within three days of its receipt convene a meeting and shall after due verification, attestation and authentication submit the case to the Office of the Inspector General of Police through the DIG/IT.
4. The DIG/IT on receipt of the case, within three days, shall place the case received from the Verification Committee before the Inspector General of Police for his approval.
5. On receiving the approval of the Inspector General of Police, the rectification or erasure, as the case may be, shall be carried out by the DIG/IT through his technical staff.

**V- EXCHANGE OF DATA AND INTERNATIONAL COOPERATION**

In order to foster national and international cooperation as per the law and as per the policy of the Government, the exchange of data related to the Gender Based Violence (GBV) cases and about safety of children shall be done by the DIG/IT in consultation with the DIG/Legal. This part of the Standing Order shall be read and interpreted to supplement the existing legal framework and shall be followed insofar as it is not inconsistent with the express provision of any law or rule.

**VI- DATA LEAK OR UNAUTHORIZED ACCESS**

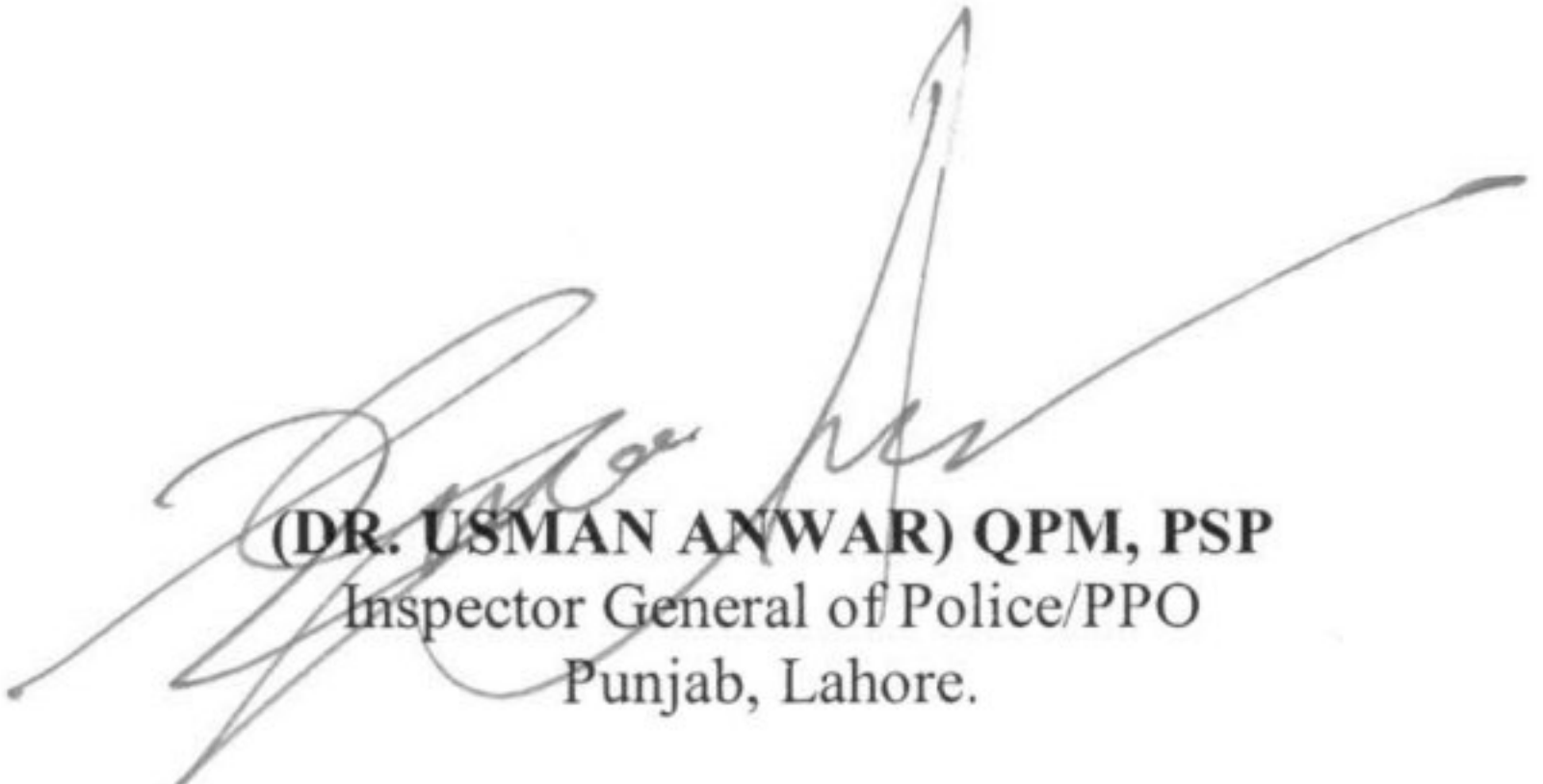
1. The officers/staff dealing with databases shall be monitored by the Heads of District Police.
2. The data leak/unauthorized usage of data shall be punished with major penalty under the disciplinary regime.
3. In case of serious breach of information/computer system, the officer/staff may be proceeded against under criminal law.

**VII- PERIODIC REVIEW**

The Standing Order shall be put to periodic review after every two years to update the instructions as per the latest technological, administrative and legal requirements.

**VIII- DATA REPORTING**

1. All the Heads of the District Police shall send complete details to DIG/Information Technology (IT), Punjab on monthly basis about all such cases wherein Police Character Certificates have been issued without entries of criminal cases in which applicant had been acquitted, discharged, FIRs quashed or prosecution withdrawn.
2. The DIG/IT, shall be responsible to maintain and update district-wise record of all such cases.

  
**(DR. USMAN ANWAR) QPM, PSP**  
Inspector General of Police/PPO  
Punjab, Lahore.