REGISTERED No. M - 302
L.-7646

The Gazette of Pakistan

EXTRAORDINARY
PUBLISHED BY AUTHORITY

ISLAMABAD, TUESDAY, AUGUST 7, 2018

PART II

Statutory Notifications (S. R. O.)

GOVERNMENT OF PAKISTAN
INFORMATION AND TELECOMMUNICATION DIVISION

NOTIFICATION

Islamabad, the 20th July, 2018

S.R.O. 979(I)/2018.—In exercise of the powers conferred by section 51 of the Prevention of Electronic Crimes Act, 2016 (XL of 2016), read with section 29 thereof, the Federal Government is pleased to make the following rules, namely:-

1. **Short title and commencement.**—(1) These rules may be called the Prevention of Electronic Crimes Investigation Rules, 2018.

(2) They shall come into force at once.

2. **Definitions.**—In these rules,—

(a) "Act" means the Prevention of Electronic Crimes Act, 2016 (XL of 2016);

(b) "Additional Director" means Additional Director of Cybercrime Wing of the Federal Investigation Agency;

Price: Rs. 100.00

[7018 (2018)/Ex. Gaz.]

(c) "Additional Director General" means Additional Director General of Cybercrime Wing of the Federal Investigation Agency;

(d) "authorized officer" means an officer of the investigation agency authorized by the Director General to perform any function of the authorized officer under the Act and the rules;

(e) "case property" means an item seized during investigation;

(f) "circle in-charge" means the overall in-charge of each Cyber Crimes Reporting Center of a Cybercrime Wing;

(g) "Code" means the Code of Criminal Procedure, 1898 (Act V of 1898);

(h) "complainant" means a person who makes a complaint for legal action under the Act;

(i) "Cybercrime Reporting Center" means a center established by the Investigation Agency for dealing with the matters under the Act within specified territorial limits;

(j) "Cybercrime Wing" means the Cybercrime Wing of the Federal Investigation Agency;

(k) "Director" means Director of Cybercrime Wing of the Federal Investigation Agency;

(l) "Director General" means Director General of the Federal Investigation Agency;

(m) "Duty Officer" means an officer of the Federal Investigation Agency not below the rank of Assistant Sub-Inspector at the helpdesk of the Cybercrime Wing of the Federal Investigation Agency;

(n) "investigation agency" means the Federal Investigation Agency established under the Federal Investigation Agency Act, 1974 (VIII of 1975);

(o) "investigation officer" means the authorized officers of the investigation agency assigned to investigate complaints within the Cybercrime Wing of the Federal Investigation Agency;

(p) "Schedule" means a schedule to these rules; and

(q) "zone" means an area having a maximum of three Cybercrime Reporting Centers in it.

3. **Investigation agency.**—(1) The Federal Investigation Agency is designated as the investigation agency for investigation of offences under the Act and shall discharge its functions under the Act and the rules through the Cybercrime Wing under the supervision of the Director General.

(2) Subject to sub-rule (3), the circle-in-charge shall act as the authorized officer for the purposes of registration of a complaint and conducting an investigation and exercising any ancillary powers under the Act.

(3) The Additional Director General may assign cases to any suitable officer of the Cybercrime Wing for investigation under the Act.

4. **Cybercrime Wing.**—(1)The Cybercrime Wing shall be manned by such personnel, having qualifications and skills in the relevant subjects including computer science, digital forensics, information technology, telecommunications, computer engineering, law or a related field to generate forensic reports, investigate and prosecute offences under the Act, as specified in Schedule I.

(2) The Cybercrime Wing shall be headed and supervised by an Additional Director General who shall be assisted by Directors and Additional Directors to be appointed by the Director General for respective zones.

(3) The Cybercrime Wing shall be organized into:

(a) investigation section;

(b) forensics section; and

(c) data and network security section.

(4) The investigation section shall be responsible for conducting investigations on complaints under the Act.

(5) The forensic section shall perform the duties of conducting forensic analysis and retrieval of digital evidence from the electronic equipment.

(6) The data and network security section shall be responsible for joint analysis and investigation of cases relating to internet, network data and systems.

(7) The organizational structure of the Cybercrime Wing shall be as provided in Schedule II.

(8) The Federal Investigation Agency, in addition to the Cybercrime Reporting Centers and forensic laboratories notified under Schedule III, may establish, with the prior approval of the Ministry of Interior, further Cybercrime Reporting Centers and forensic laboratories at such places as may be deemed necessary.

(9) The circle in-charge shall manage and control the Cybercrime Reporting Center.

(10) An officer not below the rank of Assistant Director shall manage and control the cybercrime helpdesk at the Cybercrime Reporting Center.

(11) A Deputy Director Forensics having qualification and experience in digital forensics, information security and related fields as provided in the Schedule II shall manage and control the cybercrime forensic laboratory.

(12) An Additional Director in a zone shall supervise a maximum of three Cybercrime Reporting Centers and forensic laboratories and shall work under the direct supervision of the Director Operation.

(13) The Director General shall ensure fair representation of women in the Cybercrime Wing and at least twenty five percent of investigation and helpdesk officers at the Cybercrime Reporting Centers shall be women.

5. **Powers, functions and responsibilities of cybercrime officers.**—(1) The Director General shall be responsible for overall administration of the Cybercrime Wing and authorized to exercise the powers of the investigation agency under the Act.

(2) Subject to any limitations or requirements provided under the Act or the Code, the authorized officers shall, for the purpose of an investigation under the Act, in their area of jurisdiction, have such powers, including powers relating to search and seizure of property, arrest of persons, and such duties and responsibilities as the officers of a police station have in relation to the investigation of offences under the Code.

(3) The authorized officer may, for the purposes of any investigation under the Act, exercise any of the powers of an officer in-charge of a police station under the Code in any area in which he is for the time being in relation to investigation of an offence under the Act and, when so exercising such powers, shall be deemed to be an officer in-charge of a police station discharging his functions as such within the limits of his police station.

6. **Cybercrime complaint registration.**—(1) The Cybercrime Wing shall establish helpdesks, comprising of duty officers under the supervision of circle in-charge at all Cybercrime Reporting Centers.

(2) A complaint management and tracking system shall be installed at the cybercrime headquarters and all the Cybercrime Reporting Centers to digitalize registration and expedite processing of cyber complaints which shall provide a platform of centralized database of complaints, digitally connected with all the Cybercrime Reporting Centers.

(3) A complainant may file the complaint in-person, via email, fax, telephone or other available digital means to a Cybercrime Reporting Center.

7. **Investigation and case procedure.**—(1) The circle in-charge may allow registration of a case on a complaint and nominate an investigation officer.

(2) The investigation officer shall conduct the investigation on a clearly chalked out investigation work plan which shall be approved by the circle in-charge as specified in Schedule IV.

(3) The investigation officer shall submit an investigation report within sixty days from the date of registration of a case as specified in Schedule IV.

(4) In case a cognizable offence has been committed under the Act, the circle in-charge, after seeking legal opinion, shall order the registration of such case subject to the prior approval of Additional Director in the zone.

(5) In case of a non-cognizable offence under the Act, the circle in-charge shall seek permission of the competent Court for investigation under section 155 of the Code.

(6) Notwithstanding the requirement to file an interim challan, the Additional Director in a zone shall authorize the submission of final challan under section 173 of the Code.

8. **Search and seizure.**—(1) The investigation officer shall conduct search and seizure, strictly in accordance with the provisions of the Act and where required by the Act, after obtaining prior warrant from the Court.

(2) Upon seizure of case property, the proper chain of custody and integrity of seized articles shall be maintained in line with the procedure laid under the Act and specified in Schedule V.

(3) While conducting any search or seizure, the investigation officer shall ensure that only such data or equipment is seized that is absolutely necessary for investigation of the case and search or seizure is conducted strictly in accordance with the provisions of the Act and the Code.

(4) The investigation officer shall thoroughly process the crime scene by ensuring its integrity, security and proper documentation of seized items and

shall prepare a crime scene sketch and video record and photograph the crime scene and seized items.

(5) Any search or seizure conducted in violation of the Act or the Code, shall amount to misconduct and render the concerned officer, in addition to any other liability, to disciplinary action.

9. **Investigation of offences against modesty and dignity of natural persons.**—(1) In addition to the requirements of confidentiality under the Act, the investigation officer shall investigate offences against modesty and dignity of natural persons with due regard to the privacy rights of the aggrieved persons and shall not disclose the identity of the aggrieved person and the accused unless such disclosure is required by law or in in the interest of further investigation.

(2) Any unauthorized disclosure of the contents relating to the modesty and dignity of natural persons or tempering of digital evidence shall amount to misconduct and render the concerned officers to disciplinary action as per relevant rules of the investigation agency.

(3) The investigation officer shall facilitate the aggrieved persons to seek removal, destruction of or blocking access to information against the dignity or modesty of a natural person by the Authority.

10. **Transfer of investigation.**—(1) The Additional Director of the concerned zone may, for reasons to be recorded in writing, order transfer of any investigation within the zone if such transfer is deemed necessary in the interest of fair investigation or may forward the case to the Additional Director General for transfer of the investigation to another zone.

(2) The Additional Director General may, for reasons recorded in writing, pass the order for transfer of investigation on a request received under sub-rule (1).

(3) Any party aggrieved from an order of the Additional Director or Additional Director General may make a representation to the officer next in rank of the investigation agency who shall pass such orders including an order setting aside the order complained of or modifying the order as deemed just in the peculiar circumstances of the case.

(4) Nothing contained in this rule, an investigation in a case shall not be transferred for more than two transfers.

11. **Forensic capability.**—(1) The Cybercrime Wing shall establish and maintain forensic capabilities in line with the highest standard of working to acquire, assess and report digital evidence admissible in evidence before any Court.

(2) The Cybercrime Wing shall build the capacity of analyzing information systems, data and devices in a manner that protects and preserves the evidence and helpful in gathering of evidence.

(3) The digital evidence acquired through forensic experts shall be thoroughly assessed with respect to scope of the case to determine appropriate course of action.

(4) The forensic experts examining the digital evidence shall be duly qualified and responsible for complete and accurate reporting of the results of the digital evidence analysis including the recording steps taken during the examination.

(5) The management and working of digital forensic laboratory shall be governed under clearly defined procedures as specified under Schedule V.

12. **Expert opinion.**—(1) A digital forensic expert of Cybercrime Wing shall conduct forensic analysis of evidence and provide expert opinion in the manner as specified in Schedule VI.

(2) An expert opinion shall carry the name and designation of the expert who conducted the examination.

(3) A forensic expert entrusted with the examination of a digital evidence shall report its findings within fifteen days from the date of submission of such request and any extension of time, if required, shall be requested through the Lab Supervisor to the Additional Director General.

13. **Re-examination of digital forensic.**—(1) A person affected by an expert opinion may for a sufficient cause, apply for re-examination before the Additional Director General.

(2) If the Additional Director General is satisfied with the request for re-consideration of opinion, he may direct any other zonal forensic laboratory of the Cybercrime Wing to re-examine the digital material.

(3) The Director General may, on application of an affected person, allow second re-examination of the digital material.

14. **Standard operating procedures and guidelines.**—The Additional Director General may, from time to time, issue such operational procedures and guidelines for observance by the authorized officers during investigation, forensic analysis and prosecution of offences, as deemed appropriate in conformity with the provisions of the Act, the Code and these rules.

15. **Mandatory training courses.**—(1) The Federal Investigation Agency shall provide the following mandatory training courses to the personnel of the Cybercrime Wing:

(a) Basic Training Course for all newly recruited officers of twenty six weeks.

(b) Cyber investigation, network security and cyber research Course for cybercrime investigators, network security and research officers of ten weeks.

(c) Digital Forensic Course for the forensic laboratory personnel of ten weeks.

(d) Legal Expert Course for assistant directors and deputy directors legal of ten weeks.

(e) Circle or Zone Management Course for circle in-charges and zonal officers of ten weeks.

(f) Advanced School Course for Assistant Directors aspiring to be promoted as Deputy Directors of twelve weeks.

(2) The Additional Director General shall prepare and regularly update training modules for mandatory training courses.

(3) All training courses shall be conducted at the training academy of Federal Investigation Agency or any other training facility authorized by the Director General.

16. **Appointment, promotions and transfer.**—(1) The Cybercrime Wing shall be treated as a specialized cadre and only personnel who meet the required qualifications and criteria as specified in Schedule I shall be posted in the Wing.

(2) The Federal Investigation Agency shall arrange for regular training of its personnel and shall have a promotion policy based on performance, experience, mandatory training and advanced skills in handling of offences under the Act.

(3) The appointment, promotion and transfer of personnel of the Cybercrime Wing shall be conducted as a separate cadre under the Civil Servants (Appointment, Promotion and Transfer) Rules 1973.

17. **Joint investigation team.**—(1) The Federal or a Provincial Government on its own or at the request of the investigation agency may constitute one or more joint investigation teams, comprising of representatives from the

Cybercrime Wing, intelligence and other Government or public sector organizations or agencies.

(2) The joint investigation team shall be notified with its complete composition and the timeframe within which it shall submit its investigation report under the Act.

(3) A joint investigation team shall be comprised of the following:

(a) one or more officers of the Cybercrime Wing not below the rank of BS-19;

(b) one or more officers of an intelligence agency not below the rank of BS-18 or equivalent; and

(c) one or more police officers not below the rank of BS-18.

(4) The Cybercrime Wing shall seek and extend support and cooperation to other intelligence and Government or public sector organizations or agencies for investigation and prosecution of offences under the Act.

(5) The joint investigation team shall work on clearly defined terms of reference as provided in Schedule VII.

(6) If the Federal and a Provincial Government have separately constituted joint investigation teams for investigation of a particular case, only the joint investigation team constituted by the Federal Government shall investigate the case.

18. **Cooperation with foreign government, international organization or agency.**—(1) The Federal Investigation Agency shall be the designated agency for extending or requesting international cooperation under the Act and may fully utilize the International Criminal Police Organization (INTERPOL) for extending or seeking international cooperation in cybercrime related cases.

(2) Subject to the provisions of the Act, the Cybercrime Wing may seek or extend cooperation to any foreign government, international organization or agency, through the Ministry of Interior for investigation of an offence under the Act.

19. **Report to the Parliament.**—(1) In compliance with section 53 of the Act, the Additional Director General shall, through Ministry of Interior, submit a half yearly report to both Houses of the Parliament in respect of the activities of the Cybercrime Wing in the form specified in Schedule VIII by 31st January and 31st July regarding preceding half of the year.

(2) The Cybercrime Wing shall designate officers for regular compilation and validation of data as per the requirements of Schedule VIII.

(3) The Cybercrime Wing shall not provide any identity information in the report but it may, upon requisition of the Members of the Parliament, discuss the said report in-camera and provide identity information for examination in public interest.

(4) The Cybercrime Wing shall comply with the recommendations of the Parliament approved during consideration of the report in order to improve its functions under the Act.

20. **Principles and values of investigation.**—(1) The Cybercrime Wing shall comply with the investigation principles and values, provide clear direction and guidelines to the cybercrime investigators to protect the rights of all parties in a complaint and ensure natural justice, due process and procedural fairness during the course of investigation.

(2) The principles and values of investigation shall provide the fundamental standards for cybercrime investigations including the following:

(a) investigators should perform all investigative activities with the highest level of integrity;

(b) persons responsible for the conduct of an investigation shall demonstrate the highest professional competence;

(c) investigators should maintain impartiality, objectivity and fairness throughout investigation and shall declare any potential or real conflict of interest;

(d) investigators should endeavour to maintain both the confidentiality and the protection of witnesses;

(e) conduct of the investigation should demonstrate the investigator's commitment to ascertaining the facts of the case;

(f) findings should be based on substantiated facts and related analysis, not suppositions or assumptions and the findings shall be factual, impartial, objective and clear, and may include reasonable inference; and

(g) conclusion provides summary of the investigation based on the established facts and how they relate to the allegations and applicable law.

SCHEDULE I

[See rules 4(1) and 16(1)]

JOB DESCRIPTION AND QUALIFICATIONS

1. ADDITIONAL DIRECTOR GENERAL (BPS-21)

Job description

(i) Responsible to administer, supervise all activities of Cybercrime Wing and to control and investigate Cyber Crimes.

(ii) Undertake necessary measures to ensure implementation of cyber law and to provide guidelines to various government agencies to secure their computer networks.

(iii) Responsible to initiate appropriate measures to safe guard digital national assets and to respond cyber threats in a professional way.

(iv) Exercise all administrative and financial powers, within the framework approved by the Government for efficient working of Digital Forensic Laboratory and Cyber Crimes Reporting Centers.

Education and experience

MA, MSc(CS), BCS, BS(CS), MCS, BIT, MIT or BE Computer Engineering or LL.B with twenty years or above experience of working in the versatile areas of administration, policing, investigations, information security and network security at any relevant department or agency at senior positions. Should have sound understanding of the working of Government or public sector organizations in Pakistan, their business processes, functional areas and sufficient knowledge of regulatory bodies and their issues in Pakistan in the areas of telecom. Experience in digital forensics and sound understanding of global issues and resources dealing with information security would be preferred. Candidate having a dynamic personality with administrative capabilities and experience would be considered as additional advantage.

2. DIRECTOR (BPS-20)

Job description

(i) Responsible to administer and supervise all activities of Cybercrime Wing to control and investigate cybercrimes.

(ii) Undertake necessary measures to ensure implementation of cyber law and will provide guidelines to various government agencies to secure their computer networks.

(iii) Responsible to initiate appropriate measures to safe guard digital national assets and to respond cyber threats in a professional way.

(iv) Exercise all administrative and financial powers, within the framework approved by the Government for efficient working of Digital Forensic Laboratory, and Cybercrime Reporting Center.

Education and experience

MA, MSc(CS), BCS, BS(CS), MCS, BIT, MIT, BE Computer Engineering or LL.B with twenty years or above experience of working in the versatile areas of administration, policing, investigations, information security and network security at any relevant department or agency at senior positions. Should have sound understanding of the working of Government or public sector organizations in Pakistan, their business processes, functional areas and sufficient knowledge of regulatory bodies and their issues in Pakistan in the areas of telecom. Experience in digital forensics and sound understanding of global issues and resources dealing with information security would be preferred. Candidate having a dynamic personality with administrative capabilities and experience would be considered as additional advantage.

3. **ADDITIONAL DIRECTOR OPERATIONS/CRIMES (BPS-19)**

Job description

(i) Manage and participate in the development and implementation of goals, organization's objectives, policies, recommend and administer policies and procedures in the changing trend of Cybercrimes.

(ii) Monitor performance of technical teams of Cybercrime Reporting Centres, forensic Labs and data and network security sections and submission of performance reports to Director.

(iii) Work as zonal in-charge and supervise Cybercrime Reporting Centres and Forensic Labs.

(iv) Submit crime activity report to Director on monthly basis or as and when desired.

(v) Prepare requests for proposals related to tasks areas and implement review process.

(vi) Processing and monitoring of circle and zonal offices performance. Management of crime data of Cybercrime Reporting Centres.

(vii) Plan, direct, coordinate, and review the work plan for assigned staff including those with extended hours and 24/7 operations. Ability to fill multiple roles at the same time.

(viii) Authorized to grant permission for registration, close or re-open of investigation.

(ix) Authorized for grant of permission to register a case or FIR and submission of challan in the Court.

(x) Look after all matters relating to administrative affairs. Provide a variety of support services as and when directed by the Director.

(xi) Perform miscellaneous related duties as assigned by the Director.

(xii) Act as Drawing and Disbursement Officer for the zone.

Education and experience

MSc(CS), BCS, BS(CS), MCS, BIT, MIT, BE Computer Engineering or LL.B with fifteen years or above post qualification experience including four years in the field of cybercrime investigation, forensic, network security, research, database plus.Government or public sector organizations related work experience would be considered as an additional advantage.

4. **DEPUTY DIRECTOR INVESTIGATION/CRIME (BPS-18)**

Job description

(i) Manage and participate in the development and implementation of goals, organization's objectives, policies, recommend and administer policies and procedures in the changing trend of cybercrimes. Work as circle in-charge and supervise Cybercrime Reporting Center.

(ii) Conduct all investigations, collection and preservation of evidence at the crime scene.

(iii) Prepare requests for proposals related to tasks areas and implement review process.

(iv) Processing and monitoring of circle performance. Management of crime data of Cybercrime Reporting Center.

(v) Conduct criminal investigations, identify and arrest criminals to secure the best evidence through investigation.

(vi) Prepare and execute investigation work plan.

(vii) Responsible for the collection of all relevant documentation, information or data that will be required to form an overall picture of the circumstances of the case.

(viii) Identify appropriate witnesses and obtain statements.

(ix) Submit complete and correct paperwork compiled observing highest professional standards, within set time limits and ensure evidential integrity.

(x) Command, direct and lead to subordinates when working in groups.

(xi) Assign subordinates duties, as need dictates.

(xii) Look after all matters relating to administrative affairs.

(xiii) Provide a variety of support services as and when directed by the Director.

(xiv) Perform miscellaneous duties as assigned by the Director.

Education and experience

BS(CS), BS(SE), BS (Telcom), BIT, MIT, MSc, MCS or MS(CS) with six yearsor above experience in the field of cyber investigation, network security systems and forensic analysis tools and techniques is essential. Government or public sector organizations related working experience in Pakistan and sound understanding of global interests and resources would be considered as additional advantage.

5. **DEPUTY DIRECTOR ADMIN (BS-18)**

Job description

(i) Maintain training of employees; maintaining a safe and secure work environment; developing personal growth opportunities.

(ii) Initiate, coordinate and enforcing systems, policies and procedures.

(iii) Recommend or order transfer or posting of the employees.

(iv) Deal with all kind of logistic matters.

(v) Plans, directs and manages the operation of a very large sized operation, or directs a complex specialized program.

(vi) Supervise a large diversified administrative program, which may involve coordinating the work performed in several separate locations.

(vii) Prepare reports and data of a complex nature for the department.

(viii) Design and review systems and procedures to accommodate new or additional work or to provide improved efficiency.

(ix) Supervise, train and monitor subordinate staff.

(x) Act as advisor on administrative matters to senior management and to regional offices.

(xi) Carry out special assignments for senior personnel.

(xii) Coordinate work in regional offices.

(xiii) Analyze various reports and make recommendations to senior personnel.

(xiv) Performs other duties as assigned.

Education and experience

BS(CS), BS(SE), BS (Telcom), BIT, MIT, MSc, MCS or MS(CS) with six years or above experience in the field of cyber investigation, network security systems, forensic analysis tools and techniques is essential. Government or public sector organizations related working experience in Pakistan and sound understanding of global interests and resources would be considered as additional advantage.

6. **DEPUTY DIRECTOR FORENSICS (BS-18)**

Job description

(i) Conduct examinations of computers and media generated by computers to develop evidence as an expert in the specialty area of forensic computer science.

(ii) Use experience and knowledge of a wide variety of advanced computer technologies and theories to conduct analysis of submitted evidence.

(iii) Receive, inventories, and signs for physical evidence submitted for examination.

(iv) Review laboratory requests and determines the type of examination needed.

(v) In data recovery cases, determine the most appropriate method of protecting original evidence and recovering deleted, erased, hidden and encrypted data.

(vi) With other forensic scientists and examiners, identifies and recommends methods and procedures for preservation, evidence recovery, and presentation of computer evidence.

(vii) Take proper safety precautions, anticipates unsafe circumstances, and acts accordingly to prevent accidents.

(viii) Responsible for the safety of self, others, materials, and equipment. Uses all required safety equipment.

Education and experience

PhD, MSc(CS), BCS, BS(CS), MCS, BIT, MIT,BE Computer Engineering, or Telecom Engineeringwith (three years or above post qualification for Ph.D and six years or above post qualification for MCS) experience in IT or Information Security including three years in cybercrimes investigation or computer forensic. Government or public sector organizations related working experience in Pakistan and sound understanding of global interests and resources would be considered as additional advantage.

7. **DEPUTY DIRECTOR RESEARCH (BS-18)**

Job description

(i) Drafting research specifications accordingly.

(ii) Managing external researchers and more junior staff; supervising, encouraging and mentoring.

(iii) Ensuring that research is conducted within a set time frame to meet policy requirements. Agreeing the terms of reference for research.

(iv) Liaising between external researchers and policy customers.

(v) Commenting on draft research instruments (e.g. questionnaires).

(vi) Ensuring quality control of research.

(vii) Commenting on or editing draft research reports.

(viii) Working in close partnership with both external research contractors and policy colleagues during the course of research studies.

(ix) Working on a wide range of research assignments and employing a range of different research methodologies.

(x) Producing both written and oral briefs for policy colleagues and ministers based on reviews of research evidence.

(xi) Explaining complex ideas and findings in a way that can be easily understood by lay people.

(xii) Working in an analytical, systematic and rational way.

Education and experience

MSc, (CS), BCS, BS(CS), MCS, BIT, MIT or BE Computer Engineering with (six yearsor above computing education) with three year or above experience or BCS (CS) (four years) with five yearsor above experience of working as a network security expert in a well reputed establishment or company. Strong background in information security, including program analysis, development and testing. Experience in providing information security to a complex entity.

8. **DEPUTY DIRECTOR NETWORK SECURITY (BS-18)**

Job description

(i) Participate in the security monitoring of mission-critical network nodes and systems, and security devices.

(ii) Provide second-level response and investigation to security monitoring team.

(iii) Investigate abnormal events, qualify potential security breaches, raise security incident alerts and perform technical and management escalation.

(iv) Implement second level mitigation action in response to confirmed security incidents and answer to network security experts escalations for verification and possible further mitigation actions.

(v) Perform assigned change management activities on security devices.

(vi) Document incident cases and archive all related evidence.

(vii) Write and update process and procedure or guideline documents to ensure consistent, effective and efficient methods to meet the operational goals.

(viii) Lead network security risk and vulnerability assessments and systems security audits.

(ix) On call to support 24/7 security monitoring team when required.

Education and experience

BS(CS), BS(SE), BIT, MIT, MSc(Electronics) or MSc (CS) having five years or above post qualification experience in the relevant field as a network security expert in a well reputed establishment or company.

9. **DEPUTY DIRECTOR SOFTWARE (BS-18)**

Job description

(i) Participating in the planning and Architecting and developing software and preparing technical documentation describing the usage of this software; integrating and packaging internally-and externally-developed software to provide seamless environments to users.

(ii) Deploying software and supporting its use by local and remote users.

(iii) Measuring the effectiveness of programming tools and techniques and developing new tools and techniques to use distributed resources most efficiently

Education and experience

MSc (CS), BCS, BS(CS), BS(SE), BIT or MIT having five years or above post qualification relevant experience of working as senior software developer in a well reputed establishment or company.

10. DEPUTY DIRECTOR DATABASE (BS-18)

Job description

(i) Review, develop, and design data models using standard diagramming techniques, in conjunction with application development teams; create logical data models and translate into physical database structures that integrate with existing or proposed database structures.

(ii) Monitor relational databases to optimise database performance, resource use, and physical implementation of databases; address a variety of database integration issues including migration between disparate databases, integration, maintenance/conversion, capacity planning issues, and new applications.

(iii) Monitor and maintain database security and database software, in cooperation with data security administrators and to maintain availability and integrity of databases through multiple access schemes; facilitates sharing of common data by overseeing proper key and index management and data dictionary maintenance.

(iv) Monitor and manage database backups, logs, and journals; install, maintain and upgrade database software; restore and recover data as required.

(v) Create, procure and maintain various database related documents such as manuals and programmers handbooks.

Education and experience

MSc (CS), BCS, BS(CS), BS(SE), BIT or MIT having five years or above relevant post qualification experience of working as database administrator in a well reputed establishment or company.

11. DEPUTY DIRECTOR LEGAL (BS-18)

Job description

(i) Ensuring departmental field procedures are in compliance with existing legal requirements.

(ii) Attending and providing legal counselling for cybercrime investigations.

(iii) Providing legal advice regarding the handling and disposition of evidence.

(iv) Publishing articles and summaries of legislative enactments and relevant court cases.

(v) Developing training outlines and teaching subject which have legal content; and providing on-the-spot legal advice to officers when the advice affects an active, on-going cybercrime investigation which cannot wait for research at the office.

(vi) Assists with major cybercrime investigations.

Education and experience

LL.B having seven years or above post qualification experience in the relevant field.

12. **ASSISTANT LEGAL ADVISOR (BS-17)**

Job description

(i) Ensure that departmental field procedures are in compliance with existing legal requirements.

(ii) Attend and provide legal counselling for cybercrime investigations of cybercrimes.

(iii) Prosecution of NR3C cases in Courts.

(iv) Provide legal advice regarding handling and disposition of evidence, publishing articles and summaries of legislative enactments and relevant court cases.

(v) Develop training outlines and teach subject which have legal content.

(vi) Provide on-the-spot legal advice to investigators.

Education and experience

LL.B having five years or above relevant post qualification experience or Bar-at-Law or LL.M having two years or above relevant experience in Courts.

13. **ASSISTANT DIRECTOR CYBER CRIME INVESTIGATION (BS-17)**

Job description

(i) Prepare investigation work plan for all entrusted cases and enquires.

(ii) Undertake investigation of cybercrime within the area of jurisdiction of Investigation Section, including completing actions, offender processing, preparation of evidential files and relevant court appearances.

(iii) Conduct all investigations, collection and preservation of evidence at the crime scene.

(iv) Conduct criminal enquiries and investigations, identify and arrest criminals to secure the best evidence through investigation, working to an agreed case investigation plan.

(v) Responsible for the collection of all relevant documentation, information or data that will be required to form an overall picture of the circumstances of the case.

(vi) Identify appropriate witnesses and obtain statements.

(vii) Submit complete investigation reports observing highest professional standards, within set time limits and ensure evidential integrity.

(viii) Command, direct and lead subordinates when working in groups.

(ix) Assign subordinates duties, as need dictates.

(x) Conduct departmental inquiries where entrusted.

Education and experience

MSc(CS), BCS, BS(CS), BS(Telecom), BS(SE), BIT or MIT having five years or above post qualification experience in forensics, information security, data recovery techniques. A good knowledge of network security systems, forensic analysis tools and techniques is essential. Government or public sector organizations related working experience in Pakistan and sound understanding of global interests and resources would be considered as additional advantage.

14. **ASSISTANT DIRECTOR ADMIN (BS-17)**

Job description

(i) Plans, directs and manages the operation of a very large sized operation, or directs a complex specialized program.

(ii) Supervise a large diversified administrative program, which may involve coordinating the work performed in several separate locations.

(iii) Recommend transfer or posting of the employees.

(iv) Prepare reports and data of a complex nature for the department.

(v) Design and review systems and procedures to accommodate new or additional work or to provide improved efficiency.

(vi) Supervise, train and monitor subordinate staff.

(vii) Act as advisor on administrative matters to senior management and to regional offices.

(viii) Carry out special assignments for senior personnel.

(ix) Coordinate work in regional offices.

(x) Analyze various reports and make recommendations to senior personnel.

(xi) Performs other duties as assigned.

Education and experience

MSc (CS), BCS, BS(CS), BS(Telecom), BS(SE), BIT or MIT having experience (five years or above post qualification) in forensics, information security, data recovery techniques will be eligible. A good knowledge of network security systems, forensic analysis tools and techniques is essential. Government or public sector organizations related working experience in Pakistan and sound understanding of global interests and resources would be considered as additional advantage.

15. **ASSISTANT DIRECTOR LOGISTIC (BS-17)**

Job description

(i) Preparation of master copy of invoices for each month.

(ii) Attaching invoices and other supporting documents with the voucher.

(iii) Arranging the vouchers according to ledgers in each file.

(iv) Maintaining petty cash.

(v) Updating bank register and preparing bank reconciliations.

(vi) Coordination with suppliers and preparation of procurement documents i.e. purchase requisition, goods received note etc.

(vii) Maintain inventory of office stationery etc.

(viii) Preparation of HR documents.

(ix) Maintaining personal files of the personnel.

(x) Assist Accounts officer in all kind of financial matters.

(xi) Payment of utility cheques, vendor bills etc.

(xii) Supervise office vehicle and responsible for review of vehicle log-books.

(xiii) Preparation of summary of monthly fuel expense, food expense, communication expense etc.

(xiv) Ensure logistics requirements take gender-specific needs into consideration.

(xv) Any other task assigned by the supervisors.

Education and experience

MSc(CS), BCS, BS(CS), BS(Telecom), BS(SE), BIT or MIT having five years or above post qualification experience in forensics, information security, data recovery techniques. A good knowledge of network security systems, forensic analysis tools and techniques is essential. Government or public sector organizations related working experience in Pakistan and sound understanding of global interests and resources would be considered as additional advantage.

16. **ASSISTANT DIRECTOR, STRESS COUNSELOR (BS-17)**

Job description

(i) Develop and implement a stress management plan applicable to all Cybercrime Reporting Centers in the country.

(ii) Provide individual, group and critical incident counselling sessions to the complainants or victims and dependents as/when needed.

(iii) Identify, address and follow up on critical incident stress cases among the cybercrime victims and dependents in the country.

(iv) Be willing to visit and travel regularly to the offices or sub-offices in the country in order to implement preventative stress management training activities and offer technical consultations when needed.

(v) Perform ongoing assessments and monitor the determinants of stress in complainants to include activities such as data collection, analyses and related documentation.

(vi) Conduct regular stress counselling sessions for all personnel in zonal offices, Cybercrime Reporting Centers, forensic labs and headquarters.

Education and experience

Minimum master's degree or equivalent in psycho-educational studies, psychology, psychiatry, clinical social work, or other clinical mental health profession. Minimum of five years of professional experience in psychological counselling, training skills, with special emphasis on managing critical incident stress. Female candidates would be preferred for this post.

17. **ASSISTANT DIRECTOR HARDWARE (BS-17)**

Job description

(i) Plan, design, construct and maintain the hardware equipment of computers.

(ii) Carry out repairs and testing of computer equipment and peripherals.

(iii) Ensure hardware systems are up and running at all times without interrupting the flow of work.

(iv) Recommend purchase of equipment to control dust, temperature, and humidity in areas of system installation.

(v) Specify power supply requirements and configuration.

(vi) Coordinate installation of software system.

(vii) Monitor functioning of equipment to ensure system operates properly.

(viii) Make repairs as needed.

(ix) Train users to use new or modified computer systems and equipment.

Education and experience

MSc(CS), BCS, BS(CS), BS(SE), BIT, MIT having five years or above relevant post qualification experience of working as hardware engineer in a well reputed establishment or company.

18. **ASSISTANT DIRECTOR ACCOUNTS (BS-17)**

Job description

(i) Look after all matter relating to financial affairs including preparation of papers for disbursement, maintaining accounts, complying with audit requirements and preparing reports on financial matters.

(ii) Maintain accounts and finance – related system, procedures and methods for record keeping.

(iii) Prepare a variety of reports on financial activities and status for budge preparation.

(iv) Perform miscellaneous related duties as assigned.

Education and experience

Bachelor degree in commerce, account or ACM. Minimum five years relevant post qualification experience.

19. **ASSISTANT DATABASE ADMINISTRATOR (BS-17)**

Job description

(i) Review, develop, and design data models using standard diagramming techniques, in conjunction with application development teams; create logical data models and translate into physical database structures that integrate with existing or proposed database structures.

(ii) Monitor relational databases to optimise database performance, resource use, and physical implementation of databases; address a variety of database integration issues including migration between disparate databases, integration, maintenance/conversion, capacity planning issues, and new applications.

(iii) Monitor and maintain database security and database software, in cooperation with data security administrators and to maintain availability and integrity of databases through multiple access schemes; facilitates sharing of common data by overseeing proper key and index management and data dictionary maintenance.

(iv) Monitor and manage database backups, logs, and journals; install, maintain and upgrade database software; restore and/or recover data as required.

(v) Create, procure and maintain various database related documents such as manuals and programmers handbooks.

Education and experience

MSc(CS), BCS, BS(CS), BS(SE), BIT or MIT having three years or above relevant post qualification experience of working as database administrator in a well reputed establishment or company.

20. **ASSISTANT DIRECTOR NETWORK (BS-17)**

Job description

(i) Manages multiple servers, workstations, and X terminals, ensuring proper integration of these components with existing computer systems.

(ii) Manage multiple linked databases to include security, data safety and integrity, disaster recovery, and development and implementation of bulk data import and export procedures.

(iii) Responsible to plan and implement system security policy, to include firewalls, host and client access, file permissions, and user accounts and to design and develop advanced methods and procedures for collecting, organizing, interpreting, and classifying data for input and retrieval and to design program specific applications in accordance with the needs; to install and debug new and upgraded software on server and other platforms, ensuring compliance with current site licenses; designs, programs, and manages websites and associated pages.

(iv) Research, evaluate, purchase, install, configure, and troubleshoot all hardware, peripherals, and equipment, networks, systems, and applications necessary to meet integrated systems objectives.

Education and experience

MSc(CS), BCS, BS(CS), BS(SE), BIT or MIT level having three years or above relevant post qualification experience of working as network administrator in a well reputed establishment or company.

21. **ASSISTANT DIRECTOR/IN-CHARGE HELPDESK (BS-17)**

Job description

(i) Supervise Duty officers.

(ii) Overall in-charge of complaint management and tracking system.

(iii) Monitor the complaint management system and submit the report on weekly basis to Deputy Director Crime.

(iv) Responsible to maintain complete data relevant to cases enquiries and complaints of Cybercrime Reporting Center.

(v) Responsible to assist the Deputy Director Crime.

(vi) Manage the query from organizations, public etc.

(vii) Manage the complaints received from departments, public in person or through emails, telephone or any other digital means.

(viii) Post of Help Desk Officer is re-designated as Assistant Director Help Desk Officer.

(ix) Responsible to scrutinize each complaint before submission to Investigation Officer.

Education and experience

MSc (CS), BCS, BS(CS), BS(Telecom), BS(SE), BIT or MIT having three years or above post qualification experience in the relevant field in a well reputed establishment/company.

22. **VICTIM AND WITNESS SUPPORT OFFICER (BS-17)**

Job description

(i) Contact each victim and witness to ensure victims are correctly identified and offered the appropriate level of support and decide on the best way to carry out a need assessment.

(ii) Ensure all victims and witnesses are updated with the progress of their case.

(iii) Respond to enquiries from victims and witnesses seeking progress updates, escalating any potential victim/witness problems to relevant parties. Prepare victims and witnesses for the court process and possible attendance at Courts to give evidence.

(iv) Accurately use relevant computer systems, recording and updating information to ensure an effective service is provided. Comply with time constraints, quality standards, data protection and information security requirements whilst up holding the Codes of Ethics.

(v) Maintain a process of monitoring incoming work, in order to prioritise the work being undertaken and ensure that work is being delivered in a timely manner. Deliver a high level of personal performance and actively contribute to the overall performance objectives Victims code of practice and strengthening public confidence.

(vi) Responsible for providing a point of contact with victims and witnesses of crime.

Education and experience

MSc(CS), BCS, BS(CS), BS(Telcom), BS(SE), BIT or MIT having five years or above post qualification experience in the relevant field of Forensics, Information Security, data recovery techniques will be eligible. A good knowledge of victim and witness support services and techniques is essential. Government or public sector organizations related working experience in Pakistan and sound understanding of global interests and resources would be considered as additional advantage.

23. **ASSISTANT DIRECTOR FORENSIC (BS-17)**

Job description

(i) Conduct examinations of computers and media generated by computers to develop evidence as an expert in the specialty area of forensic computer science.

(ii) Use experience and knowledge of a wide variety of advanced computer technologies and theories to conduct analysis of submitted evidence.

(iii) Receive, inventories, and signs for physical evidence submitted for examination.

(iv) Review laboratory requests and determines the type of examination needed.

(v) In data recovery cases, determine the most appropriate method of protecting original evidence and recovering deleted, erased, hidden and encrypted data.

(vi) With other forensic scientists and examiners, identifies and recommends methods and procedures for preservation, evidence recovery, and presentation of computer evidence.

(vii) Take proper safety precautions, anticipates unsafe circumstances, and acts accordingly to prevent accidents.

(viii) Responsible for the safety of self, others, materials, and equipment. Uses all required safety equipment.

(ix) Technical writing written and oral communications skills organizational and multi-tasking abilities Results and deadline-oriented skills.

(x) Responsible for writing and editing standard operating procedures, laboratory procedure manuals, and other related documents.

Education and experience

MSc(CS), BCS, BS(CS), MCS, BIT, MIT or BE Computer Engineering, Telecom Engineering six years or above post qualification experience in the relevant field of IT or information security including three years or above experience in cybercrimes investigation or computer forensic. Government or public sector organizations related working experience in Pakistan and sound understanding of global interests and resources would be considered as additional advantage.

24. **INSPECTOR - CYBER CRIME INVESTIGATOR (BS-16)**

Job description

(i) Prepare investigation work plan for all entrusted cases and enquires.

(ii) Undertake investigation of cybercrime within the area of jurisdiction of Investigation Section, including completing actions, offender processing, preparation of evidential files and relevant court appearances.

(iii) Conduct all investigations, collection and preservation of evidence at the crime scene.

(iv) Conduct criminal enquiries and investigations, identify and arrest criminals to secure the best evidence through investigation, working to an agreed case investigation plan.

(v) Responsible for the collection of all relevant documentation, information or data that will be required to form an overall picture of the circumstances of the case.

(vi) Identify appropriate witnesses and obtain statements.

(vii) Submit complete investigation reports observing highest professional standards, within set time limits and ensure evidential integrity.

(viii) Command, direct and lead subordinates when working in groups.

(ix) Assign subordinates duties, as need dictates.

Education and experience

MSc (CS), BCS, BS(CS),BS(Telecom), BS(SE), BIT or MIT having five years or above post qualification experience in the relevant field of forensics, information security, data recovery techniques will be eligible. A good knowledge of network security systems, forensic analysis tools and techniques is essential. Government or public sector organizations related working experience in Pakistan and sound understanding of global interests and resources would be considered as additional experience.

Minimum physical standard

For male candidates: Height 5'-6" and Chest 32"-33 1/2".

For female candidates: Height 5'-2"(documentary proof from authorized Medical authorities required).

25. **CYBER CRIME ANALYST (BS-16)**

Job description

(i) The analyst will provide tactical and strategic analysis through the investigation of suspicious network and account activity that could lead to data or monetary loss. The analyst will be expected to report

cybercriminal tactics techniques and procedures (TTPs), trends, patterns, and emerging threats that threaten customer data and financial losses.

(ii) The analyst will leverage open sources, vendors, Clear net and Dark web data to detect and mitigate the exploitation of Discover assets that leads to data loss (customer information).

(iii) At times, the analysts will be expected to work in the absence of oversight and management.

(iv) Assist in developing strategic analysis through the identification and reporting of cybercriminal tactics techniques and procedures (TTPs), criminal trends and patterns, emerging threats and the changing fraud landscape.

(v) Assist in providing deliverables in the form of Operational Analysis, Collection reports, Threat assessments for specific crimes, Scheduled reports that include weekly and monthly reports.

(vi) Engages the organization on both technical and non-technical fraud.

(vii) Responsible for enhancing the Cyber Fraud intelligence capability as part of the cyber fraud team's mitigation efforts.

(viii) Promote a risk-aware culture and ensure efficient and effective risk and compliance management practices by adhering to required policies and procedures.

Education and experience

MSc (CS), BCS, BS(CS), BS(Telecom), BS(SE), BIT or MIT having five years or above post qualification experience in the relevant field of forensics, information security, data recovery techniques will be eligible. A good knowledge of network security systems, forensic analysis tools and techniques is essential. Government or public sector organizations related working experience in Pakistan and sound understanding of global interests and resources would be considered as additional experience.

26. **OFFICE SUPERINTENDENT (BS -16)**

Job description

(i) Record keeping of all branches or sections.

(ii) Supervise the work of Assistants, Clerks etc.

cybercriminal tactics techniques and procedures (TTPs), trends, patterns, and emerging threats that threaten customer data and financial losses.

(ii) The analyst will leverage open sources, vendors, Clear net and Dark web data to detect and mitigate the exploitation of Discover assets that leads to data loss (customer information).

(iii) At times, the analysts will be expected to work in the absence of oversight and management.

(iv) Assist in developing strategic analysis through the identification and reporting of cybercriminal tactics techniques and procedures (TTPs), criminal trends and patterns, emerging threats and the changing fraud landscape.

(v) Assist in providing deliverables in the form of Operational Analysis, Collection reports, Threat assessments for specific crimes, Scheduled reports that include weekly and monthly reports.

(vi) Engages the organization on both technical and non-technical fraud.

(vii) Responsible for enhancing the Cyber Fraud intelligence capability as part of the cyber fraud team's mitigation efforts.

(viii) Promote a risk-aware culture and ensure efficient and effective risk and compliance management practices by adhering to required policies and procedures.

Education and experience

MSc (CS), BCS, BS(CS), BS(Telecom), BS(SE), BIT or MIT having five years or above post qualification experience in the relevant field of forensics, information security, data recovery techniques will be eligible. A good knowledge of network security systems, forensic analysis tools and techniques is essential. Government or public sector organizations related working experience in Pakistan and sound understanding of global interests and resources would be considered as additional experience.

26. **OFFICE SUPERINTENDENT (BS -16)**

Job description

(i) Record keeping of all branches or sections.

(ii) Supervise the work of Assistants, Clerks etc.

(iii) Process and submit files of all branches to higher officers in proper and complete form.

(iv) Maintain the discipline and tidiness in branch or section.

Education and experience

Bachelor's degree (B.A) or B.Sc or B.Com or equivalent with minimum five years or above post qualification experience in the relevant field.

27. DATA ENTRY OPERATOR (BS-14)

Job description

(i) Do data entry of any kind within the organization.

(ii) Can be assigned to do small computer related like typing of letters, creation of mathematical sheets, creation of presentation etc.

Education and experience

FA, FSC, ICS, having three years or above relevant post qualification experience.

28. TECHNICAL ASSISTANT (BS -14)

Job description

(i) Performing technical tasks at helpdesk Cybercrime Reporting Center and digital forensic lab.

(ii) Register and enter complaints received in CMTS, at Cybercrime Reporting Center.

(iii) Proficiency with computer programs, such as Microsoft word and excel, and database systems.

(iv) Collecting and interpreting data in order to generate reports on daily basis.

(v) Reading and understand technical documentation.

(vi) Manage the query from organizations, public etc.

(vii) Manage the complaints received from departments, public in person or through emails, telephone or any other digital means.

Education and experience

BCS, BS-IT, Bachelor's degree (B.A), B. Sc, B.Com or equivalent with minimum five years post qualification experience in the relevant field of IT or relevant experience of working in a well reputed establishment or organization.

29. **SUB- INSPECTOR - CYBERCRIME INVESTIGATOR (BS-14)**

Job description

(i) Prepare investigation work plan for all entrusted cases and enquires.

(ii) Undertake investigation of cybercrime within the area of jurisdiction of Investigation Section, including completing actions, offender processing, preparation of evidential files and relevant court appearances.

(iii) Conduct all investigations, collection and preservation of evidence at the crime scene.

(iv) Conduct criminal enquiries and investigations, identify and arrest criminals to secure the best evidence through investigation, working to an agreed case investigation plan.

(v) Responsible for the collection of all relevant documentation, information or data that will be required to form an overall picture of the circumstances of the case.

(vi) Identify appropriate witnesses and obtain statements.

(vii) Submit complete investigation reports observing highest professional standards, within set time limits and ensure evidential integrity.

(viii) Command, direct and lead subordinates when working in groups.

(ix) Assign subordinates duties, as need dictates.

Education and experience

MSc (CS), BCS, BS(CS), BS(Telecom), BS(SE), BIT or MIT having five years or above post qualification experience in the relevant field of forensics, information security, data recovery techniques will be eligible. A good knowledge of network security systems, forensic analysis tools and techniques is essential. Government or public sector organizations related working experience

in Pakistan and sound understanding of global interests and resources would be considered as additional experience.

Minimum physical standard

For male candidates: Height 5'-6" and Chest 32"-33 1/2".

For female candidates: Height 5'-2"(documentary proof from authorized Medical authorities required).

30. **ASSISTANT (BS-14)**

Job description

(i) Provide comprehensive and wide ranging support or secretarial services to the senior management and the professional staff.

(ii) Order and maintain inventory or stock registers of relevant office supplies for effectiveness operations and personnel duties.

(iii) Maintain administrative, archival and personnel files.

(iv) Perform miscellaneous job-related duties as assigned.

Education and experience

Bachelor's degree (B.A) or B.Com. Minimum five years post qualification experience in the relevant field.

31. **UDC (BS-11)**

Job description

(i) Responsible for recording and indexing.

(ii) Supervise the R & I (CR) Section of the branch.

(iii) Perform night duty if required.

(iv) Prepare pay bills etc. and duty of cashier.

Education and experience

FA or FSc with three years or above post qualification experience in the relevant field. Computer experience would be preferred.

32. **ASSISTANT SUB INSPECTOR (BS-09)**

Job description

(i) Responsible to work as helpdesk officer at Cybercrime Reporting Centers.

(ii) Perform the duties as Moharrar Malkhana in zonal offices.

(iii) Perform the duties as Court Pervi Officer in zonal offices.

(iv) Perform the duties as Moharrar in zonal offices.

(v) Perform the duties as Guard-In-charge in zonal offices.

(vi) Assist the Investigators.

(vii) Responsible to handle and manage the complaints.

(viii) Responsible to perform the tasks assigned by the In-charge.

Education

F. Sc or ICS.

Minimum physical standard

For male candidates: Height 5'-6" and Chest 32"-33 1/2".

For female candidates: Height 5'-2"(documentary proof from authorized Medical authorities required).

33. **LDC (BS-09)**

Job description

(i) Deal with the routine assigned office work.

(ii) Dispatch and diaries of the office daily dak.

(iii) Provide assistance as typist.

(iv) Perform the duties as telephone operators.

Education and experience

F.A or F.Sc with two years or above post qualification experience in the relevant field.

34. **HEAD CONSTABLE (BS-07)**

Job description

(i) Perform the duties of Naib Court for assisting the prosecutor.

(ii) Provide assistance to the investigation officer for custody of the offenders.

(iii) Provide assistance during raid.

(iv) Maintain record of the seized digital equipment.

(v) Responsible to perform all duties/tasks assigned by the In-charge.

Education

FA, FSc or CS.

Minimum physical standard

For male candidates: Height 5'-6" and Chest 32"-33 1/2".

For female candidates: Height 5'-4"(documentary proof from authorized Medical authorities required).

Age: 18-25 years.

35. **CONSTABLE (BS-05)**

Job description

(i) Provide assistance to the investigation officer.

(ii) Perform assistance during raid.

(iii) Maintain record of the seized digital equipment.

(iv) Responsible to perform all duties/tasks assigned by the In-charge.

Education

Matric with science.

Minimum physical standard

For male candidates: Height 5'-6" and Chest 32"-33 1/2".

For female candidates: Height 5'-4"(documentary proof from authorized Medical authorities required).

Age: 18-25 Years

36. **DISPATCHER (BS-05)**

Job description

(i) Responsible to dispatch and deliver the dak or file within the city.

(ii) Any other duty that may be assigned to him by his officer in-charge.

Education and experience

Middle or matriculate would be given preference. Valid motorcycle driving license holder.

37. **DRIVER CONSTABLE (BS-05)**

Job description

(i) Responsible to maintain the vehicle physically.

(ii) Responsible to keep the vehicle neat and clean.

(iii) Knows defensive driving skills.

(iv) Holder of LTV driving license.

Education and experience

Matric with maximum 2nd Division, expert in driving light vehicles, valid LTV driving license, Must have knowledge of the maintenance of vehicles.

Minimum physical standard

For male candidates: Height 5'-6" and Chest 32"-33 1/2".

For female candidates: Height 5'-4"(documentary proof from authorized Medical authorities required).

Age: 18-25 years.

38. **ELECTRICIAN (BPS-05)**

Job description

(i) Maintain and operate all electrical equipment of the office.

(ii) Assist the investigators during raid to dismantle the electronic equipment's.

(iii) Install and maintain wiring, control, and lighting systems.

(iv) Diagnose malfunctioning systems, apparatus, and components, using test equipment and hand tools, to locate the cause of a breakdown and correct the problem.

Education and experience

Matric or SSC, with three years or above post qualification experience in the relevant field. Holding a valid minimum of one year diploma of electrician may be preferred.

39. **NAIB QASID (BS-02)**

Job description

(i) Clean office furniture and record before office hours.

(ii) Attend to general arrangement and tidiness of office furniture.

(iii) Carry from one place to another within and outside office premises official's files, papers or dak.

(iv) Conduct visitors to the officers.

(v) Attend to other small chores like serving of drinking water etc.

(vi) Any other duty that may be assigned to him by his Officer In charge during working hours.

Education and experience

Middle with two years or above relevant experience.

40. **SWEEPER (BS-01)**

Job description

(i) To clean office premises and other assigned areas by sweeping, mopping and scrubbing.

(ii) To clean toilet and washroom and re-stock paper and soap supplies.

(iii) To perform miscellaneous related duties as assigned.

Education and experience

At least Primary with two years or above experience in the relevant field.

SCHEDULE II

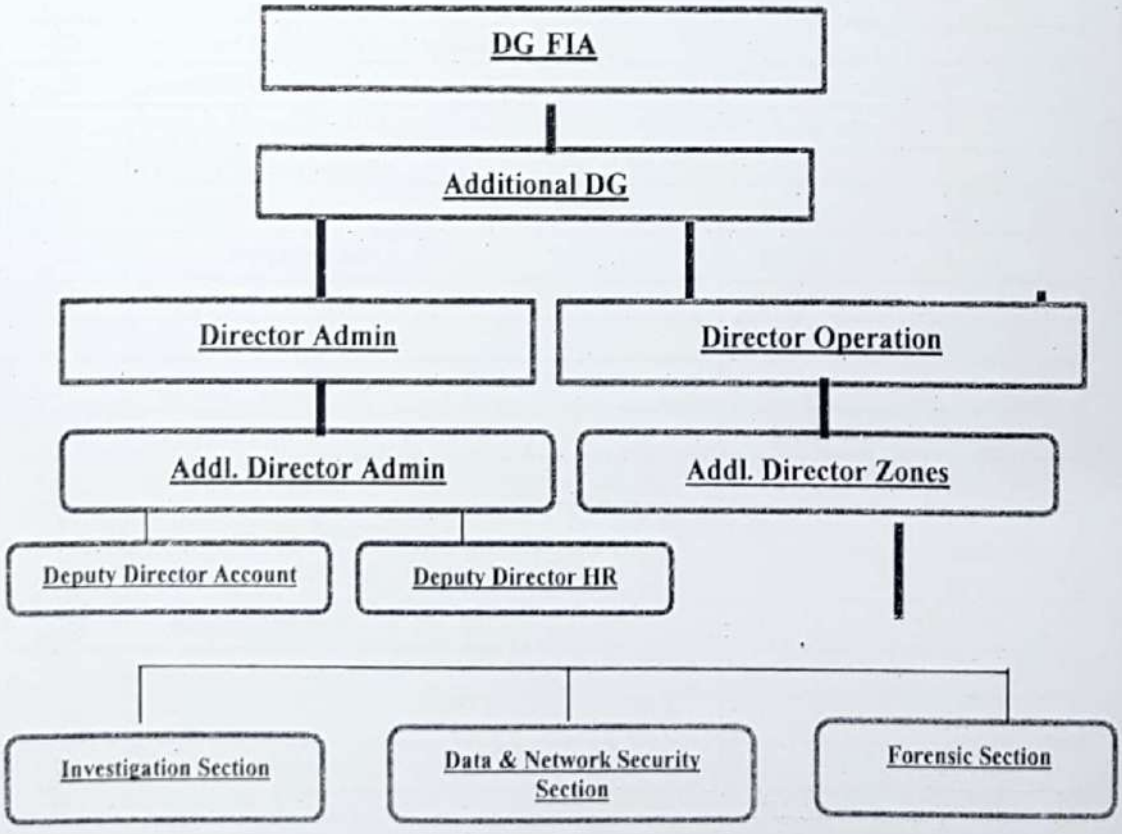
[See rules 4(7) and 4(11)]

Organizational Structure of Cybercrime Wing

The cyber-crime wing of the Federal Investigation Agency comprises of an Additional Director General's office, Directors' office/headquarters, zonal offices, cybercrime reporting centers and forensic laboratories. The organizational structure of cybercrime wing is attached as annexure A, B, C, D and E as under:

Annex-A

Organogram of Cybercrime Wing



Annex-B

Cybercrime Headquarters

Sr. No	Position	BPS	No. of Positions
1	Additional Director General	21	1
2	Director Operation	20	1
3	Director Administration	20	1
4	Additional Director Admin	19	1
5	Additional Director Crime	19	1
6	Deputy Director Crime	18	1
7	Deputy Director (R&D)	18	1
8	Deputy Director Law	18	1
9	Deputy Director Software	18	1
10	Deputy Director Network Security	18	1
11	Deputy Director Accounts	18	1
12	Deputy Director/Human Resource Officer	18	1
13	Assistant Director Accounts	17	1
14	Assistant Director Admn	17	1
16	Assistant Director Logistic	17	1
17	Assistant Director/Investigator	17	6
18	Assistant Director Stress Counselor	17	1
19	Press and Media Relations Officer	17	1
20	Victim and Witness Support Officer	17	1
21	Assistant Director (R&D)	17	1
22	Assistant Director Web	17	1
23	Assistant Network Administrator	17	1
24	Assistant Director Help Desk	17	1
25	Assistant Director Training	17	1
26	Cyber Crimes Analyst	16	2
27	Graphic Designer	16	1
28	Office Superintendent	16	1
29	Inspector Investigator	16	1
30	Inspector MTO	16	1
31	Inspector Security	16	1
32	Inspector PSO	16	1
33	Inspector Training	16	1
34	Sub- Inspector Training	16	1
35	Sub- Inspector-Investigator	14	4
36	Technical Assistant	14	4
37	Personal Assistant	14	3
38	UDC	11	5
39	Helpdesk Officer (ASI)	9	10
40	Store In-charge (ASI)	9	1

Sr. No	Position	BPS	No. of Positions
41	LDC	9	10
42	Head Constable	9	8
43	Constable	5	10
44	Dispatch Rider	5	4
45	Driver Constable	5	10
46	Naib Qasid	2	10
47	Sweeper	1	4
48	Electrician	1	1

Annex-C

Cybercrimes Zonal Office

Sr. No	Positions	BPS	Positions
1	Additional Director Zone	19	1
2	Deputy Director Zone	18	1
3	Assistant Director Accounts	17	1
4	Office Superintendent	16	1
5	Personal Assistant	14	1
6	UDC	11	1
7	LDC	9	1
8	Constable	5	12
9	Dispatcher	5	1
10	Driver Constable	5	2
11	Naib Qasid	2	2
12	Sweeper	1	2

Annex-D

Cybercrime Reporting Center

Sr. No	Position	BPS	Positions
1	Circle In-charge	18	1
2	Assistant Director/Investigator	17	10
3	Assistant Director Stress Counselor	17	1
4	Victim and Witness Support Officer	17	1
5	Cybercrime Analyst	16	2
6	Assistant Director Help Desk	17	1
7	Help Desk Officer, ASI	9	15

Sr. No	Position	BPS	Positions
8	Assistant Director Law	17	2
9	Assistant Director Network	17	1
10	Inspector-Investigator	16	8
11	Sub Inspector-Investigator	14	16
12	ASI (Moharrar Malkhana)	9	2
13	ASI (Court Pervi officer)	9	6
14	ASI (Moharrar Reporting Center)	9	2
15	ASI (Guard In-charge)	9	1
16	Head Constable	7	10
17	Constable	5	30
18	Dispatch Rider	5	2
19	Driver Constable	5	6
20	Naib Qasid	2	2
21	Sweeper	1	2

Annex-E

Digital Forensics Lab

Sr. No	Position	BPS	Positions
1	Deputy Director Forensics	18	2
2	Assistant Director Forensics	17	4
3	Assistant Director Hardware	17	1
4	Assistant Director Database	17	1
5.	Assistant Director Network	17	1
6.	Technical Assistant	14	2
7	Driver Constable	5	1
8	Security Officer(ASI)	9	4
9	Naib Qasid	2	2
10	Electrician	1	1
11	Sweeper	1	1

SCHEDULE III

[*See rule 4(8)*]

CYBERCRIME REPORTING CENTERS

Sr. No	Locations
1	Islamabad
2	Rawalpindi
3	Karachi
4	Sukkur
5	Hyderabad
6	Lahore
7	Faisalabad
8	Multan
9	Gujranwala
10	Peshawar
11	Dera Ismail Khan
12	Abbottabad
13	Quetta
14	Gwadar
15	Gilgit

SCHEDULE IV

[*See rules 7(2) and 7(3)*]

Annex – A

INVESTIGATION WORK PLAN

Case No:	
Implicated Persons:	
Investigation Plan date:	
Name of Investigator	

1. **Allegations**

(A brief summary of the reported complaint, including circumstances relevant to the matter being investigated)

2. **Applicable legal norms**

(State applicable laws (PECA 2016, PPC, etc) pertaining to the reported crime)

3. **Implicated persons**

State name(s) of persons involved in the complaint and complete address and contact details.

4. **Work Plan steps and timelines**

(I). INVESTIGATIVE ACTION

{Identify interviewees, their contact details and a tentative schedule. Also, address issues of availability, order of interviews and special needs (e.g. interpreter, guardian}

PROPOSED INTERVIEWS

No.	Name	Status (complainant, accused, witness, victim)	Contact Info (phone and e-mail)	Purpose of Interview	Tentative date/availability

(II). EVIDENCE / RECORDS PRESERVATION AND COLLECTION

{Identify known and possible sources of evidence and specify means/ process for securing those sources and collecting records – i.e. files, electronic data etc.}

COLLECTION OF EVIDENCE / RECORDS

No.	Evidence / Records to be Collected	Means of Collection/Contact Point	Date Completed

5. **Travel / mission plan**

{Proposed travel in connection with investigation - Include travel dates, length, purpose, location(s), number of investigator(s)/support required, and an estimation of costs}

6. **Resources**

(I). EQUIPMENT/INVESTIGATION TOOLS

{List required equipment for investigation, including laptop computer; portable printer; external hard drive; flash drive; digital camera; digital audio recorder; hard disk cloning software; SIM card reader/back-up; evidence bags/seals}

(II). FORENSICS / EXTERNAL EXPERTISE

{List any forensic/external support or specialized forensic equipment required for the investigation.}

Type of evidence	Explanation	Date obtained
		☐
		☐

Name and signature of assigned investigator: _____

Date:

Investigation Plan approved by: _____
(Circle in-Charge, Investigation)

Date:

Annex – B

INVESTIGATION REPORT STRUCTURE

1. **Background**

This section outlines the background of alleged complaint or the activity investigated, when and how allegations surfaced, and locations of investigations. It also provides the name and job title of the person who authorized the investigation and the terms of reference of the investigation.

2. **Persons Implicated**

This section of the report provides the details about allegations made by the complainant against the investigation subjects.

3. **Applicable Sections of Law**

This section outlines the relevant provisions of Prevention of Electronic Crimes Acts 2016 (PECA), Pakistan Penal Code (PPC) and other relevant laws on FIA schedule that have been violated.

4. **Investigation Proceedings/Methodology**

This provides methods used to undertake investigations such as interviews of witnesses, subjects, documents and evidence collected and field missions undertaken. Reports should include both exculpatory and inculpatory evidence.

If the offences under investigation are compoundable, bailable and non-cognizable or non-bailable, non-compoundable and cognizable as provided under section 43 of the Act, the investigation officer shall follow the requisite course of action in line with the relevant provisions of the Act and the Code.

5. Findings

The investigation findings provide a detailed account of the facts of the case. This section explains the investigative steps undertaken, how evidence was obtained, results of the evidence and how evidence is relevant to the allegations and conclusion of the investigation.

In short, the findings of the report:

(i) summarizes the key evidence from each witness statement

(ii) what facts have been established

(iii) what facts have not been established

(iv) whether there are any mitigating factors to consider

(v) whether there is any other relevant information to consider

6. Conclusion

Conclusion provides summary of the investigation based on the established facts and how they relate to the allegations and applicable laws. This section of the report describes as to whether or not the allegations were substantiated.

7. **Recommendations**

Recommendations should be supported by the investigative findings.

****

SCHEDULE V

[*See rule 8(2)*]

SEIZURE MEMO
(FORM – 1)

Case Number:

Item:

Date of seize:

Time:

Location:

Details of Person:

Details of Person from whom item(s) seized:

Address / Telephone Number / Email:

Description of item(s)

Description of item seized:	
Make/model:	
Serial numbers:	
Colour:	
Condition:	
Number of pages (if documents):	
Any other identifying marks:	

(Each exhibit must be supplied with its own unique identification number. Complete a separate memo for each exhibit/evidence).

	Name	Signature
Investigator		
Witness 1		
Witness 2		

CHAIN OF CUSTODY
(FORM – 2)

(Refers to the chronological documentation of each individual exhibit, showing the seizure, custody, control, transfer, analysis and disposition of evidence, physical or electronic. Every person who takes control of the item is to be recorded in the chain of custody.)

Case/ Exhibit/Seizure Number	Date / Time / Location of transfer	Description of Evidence	Delivered by	Received by

SCHEDULE VI

[*See rule 12(1)*]

Management and Working of Digital Forensic Laboratory

1. **Introduction**

Digital forensics is the science of acquiring, retrieving, preserving and presenting data that has been processed electronically and stored on digital media. It employs specialized techniques for recovery, authentication and analysis of electronic data in corporate, civil, and criminal cases. Under section 29 of the Act, the digital forensic laboratory is the facility that provides these examinations. Specialized hardware and software products are utilized in investigation of computer system, electronic devices, or any device that contain a processor and memory in order to determine the who what where when and how issues of usage.

In order to ensure evidence is not destroyed or compromised in any way, forensic experts must be careful not to handle the evidence more than necessary, as over handling can possibly change the data. Moreover, the data gathered is rarely analyzed on the same machine from which it was obtained. Experts should be on the lookout for traps such as intrusion detection devices and self-destruct mechanisms installed on digital devices by the suspects of crimes as countermeasures against forensic practices. E-mail review is another technique by the experts to gather large amounts of digital evidence that could be in the body of the message or in attachments.

2. Responsibilities

2.1 Digital Lab Supervisor

The Digital Forensic Laboratory of Cybercrime Wing shall be managed and supervised by a Deputy Director Forensics who acts as the Technical Supervisor for this section. His/her responsibilities include, but are not limited, to administrative, supervisory, and the operational functions of the Digital Forensic Laboratory section. The major responsibilities of supervisor may include:

(i) acting as a senior forensic expert for the Lab.

(ii) ensuring that new personnel are trained to meet the section's quality standards.

(iii) conducting annual performance reviews of Lab personnel.

(iv) Performing administrative/technical reviews of case records submitted by Lab personnel.

(v) administering competency and proficiency tests to Lab personnel.

(vi) ensuring hardware, software and equipment are in proper working conditions.

(vii) ensuring that all quality standards are met as required for the section. approving validation studies on hardware and software used for forensic casework.

(viii) recommending software and hardware to be implemented in the laboratory.

2.2 Digital Forensic Expert

A Digital Forensic Expert is a staff member who is authorized to examine digital evidence in assigned case work. Contingent on training and authorization, the duties of an expert may include the following:

(i) perform extraction and recovery of digital data from electronic devices.

(ii) write impartial test reports with details pertaining to their extraction and/or recovery of digital data.

(iii) perform technical and administrative reviews of submitted case records.

(iv) respond to on-scene incident call outs and assist cyber investigators in identifying devices that may contain evidence.

(v) provide expert testimony in court.

(vi) provide training and mentor guidance to new personnel.

(vii) ensure hardware, software and equipment is in proper working conditions.

(viii) conduct performance checks on software and hardware to be used for forensic casework.

3. **Digital Forensic Lab Standards**

The application and interpretation of applicable Lab standards to the digital forensics discipline requires both practical and realistic solutions. Some of the required standards may include:

(i) New technical procedures must be validated to prove their efficacy in examining evidence material before being implemented on casework.

(ii) Controls and standard samples must be used and documented in the case record to ensure the validity of the testing parameters and, thereby, the conclusion.

(iii) Instruments/equipment should be adequate and properly maintained for the procedures used.

(iv) Instruments/equipment must be properly calibrated and calibration records maintained for all calibrated instruments.

(v) Forensic personnel must qualify as expert witnesses in computer evidence processing.

(vi) Personnel must be trained in computer evidence processing procedures.

(vii) A training program to develop the technical skills of personnel is essential in each applicable functional area. Personnel must be trained on multiple tool types.

(viii) Multiple sets of tools must be available for digital examinations.

(ix) Personnel must have sufficient depth to handle multiple cases.

(x) Experts must be certified.

(xi) Internal forensics capabilities must meet potential legal challenges.

(xii) Digital processing power and media storage must be state-of-the-art.

(xiii) Evidence must be protected and accessible to only authorized personnel.

(xiv) The chain-of-custody must be maintained and documented.

4. Digital Forensic Examination Process

In order to achieve scientifically reliable and legally acceptable results in digital forensics, the cybercrimes forensic laboratory of FIA employs following four phases examination process:

(i) Assessment

(ii) Acquisition

(iii) Examination

(iv) Documentation and Reporting

5. Evidence Assessment

5.1 Principle

The digital evidence should be thoroughly assessed with respect to the scope of the case to determine the course of action.

5.2 Procedure

Conduct a thorough assessment by reviewing the search warrant or other legal authorization, case detail, nature of hardware and software, potential

evidence sought, evidence items are sealed or not, condition of evidentiary item and the circumstances surrounding the acquisition of the evidence to be examined.

5.3 **Case assessment**

Review the case investigator's request for service.

(i) Identify the legal authority for the forensic examination request.

(ii) Ensure there is a completed request for assistance.

(iii) Complete documentation of chain of custody.

Consult with the case investigator about the case and let him/her know what the forensic examination may or may not discover. When talking with the investigator about the facts of the case, consider the following:

(i) Discuss whether other forensic processes need to be performed on the evidence (e.g., search key words, tool marks, trace, and questioned documents).

(ii) Discuss the possibility of pursuing other investigative avenues to obtain additional digital evidence (e.g., sending a preservation order to an Internet service provider (ISP), identifying remote storage locations, obtaining e-mail).

(iii) Consider the relevance of peripheral components to the investigation. For example, in forgery or fraud cases consider non-computer equipment such as laminators, credit card blanks, check paper, scanners, and printers.

(iv) Determine the potential evidence being sought (e.g., photographs, spreadsheets, documents, databases, financial records).

(v) Determine additional information regarding the case (e.g., aliases, e-mail accounts, e-mail addresses, ISP used, names, network configuration and users, system logs, passwords, user names). This information may be obtained through interviews with the system administrator, users, and employees.

(vi) Assess the skill levels of the computer users involved. Techniques employed by skilled users to conceal or destroy evidence may be more sophisticated (e.g., encryption, booby traps, steganography).

(vii) Prioritize the order in which evidence is to be examined.

(viii) Determine if additional personnel will be needed.

(ix) Determine the equipment needed.

The assessment might uncover evidence pertaining to other criminal activity (e.g., money laundering in conjunction with narcotics activities).

6. Evidence Acquisition

6.1 Principle

Digital evidence, by its very nature, is fragile and can be altered, damaged, or destroyed by improper handling or examination. For these reasons special precautions should be taken to preserve this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion.

6.2 Procedure

Acquire the original digital evidence in a manner that protects and preserves the evidence. The basic steps include as under:

(i) Secure the original digital evidence through making bit by bit imaging of the evidence.

(ii) Document hardware and software configuration of the examiner's system.

(iii) Verify operation of the examiner's computer system to include hardware and software.

(iv) Disassemble the case of the computer to be examined to permit physical access to the storage devices.

(v) Take care to ensure equipment is protected from static electricity and magnetic fields.

(vi) Identify storage devices that need to be acquired. These devices can be internal, external, or both.

(vii) Document internal storage devices and hardware configuration.

(viii) Drive condition (e.g., make, model, geometry, size, jumper settings, location, drive interface).

(ix) Internal components (e.g., sound card; video card; network card, including media access control (MAC) address; personal computer memory card international association (PCMCIA) cards).

(x) Disconnect storage devices (using the power connector or data cable from the back of the drive or from the motherboard) to prevent the destruction, damage, or alteration of data.

(xi) Retrieve configuration information from the suspect's system through controlled boots.

(xii) Perform a controlled boot to capture CMOS/BIOS information and test functionality.

(xiii) Boot sequence (this may mean changing the BIOS to ensure the system boots from the floppy or CD-ROM drive).

6.3 **Date and time capture.**

(i) Perform a second controlled boot to test the computer's functionality and the forensic boot disk.

(ii) Ensure the power and data cables are properly connected to the floppy or CD-ROM drive and ensure the power and data cables to the storage devices are still disconnected.

(iii) Place the forensic boot disk into the floppy or CD-ROM drive. Boot the computer and ensure the computer will boot from the forensic boot disk.

(iv) Reconnect the storage devices and perform a third controlled boot to capture the drive configuration information from the CMOS/BIOS.

(v) Ensure there is a forensic boot disk in the floppy or CD-ROM drive to prevent the computer from accidentally booting from the storage devices.

(vi) Drive configuration information includes logical block addressing (LBA); large disk; cylinders, heads, and sectors (CHS); or auto-detect.

6.4 **Power system down.**

(i) Whenever possible, remove the subject storage device and perform the acquisition using the examiner's system. When attaching the

subject device to the examiner's system, configure the storage device so that it will be recognized.

(ii) Exceptional circumstances, including the following, may result in a decision not to remove the storage devices from the subject system.

(iii) RAID (redundant array of inexpensive disks). Removing the disks and acquiring them individually may not yield usable results.

(iv) Laptop systems. The system drive may be difficult to access or may be unusable when detached from the original system.

(v) Hardware dependency (legacy equipment). Older drives may not be readable in newer systems.

(vi) Equipment availability. The examiner does not have access to necessary equipment. Network storage. It may be necessary to use the network equipment to acquire the data. When using the subject computer to acquire digital evidence, reattach the subject storage device and attach the examiner's evidence storage device (e.g., hard drive, tape drive, CD-RW, MO).

(vii) Ensure that the examiner's storage device is forensically clean when acquiring the evidence. Write protection should be initiated, if available, to preserve and protect original evidence.

Note: The examiner should consider creating a known value for the subject evidence prior to acquiring the evidence (e.g., performing an independent cyclic redundancy check (CRC), hashing).

(i) Depending on the selected acquisition method, this process may already be completed. If hardware writes protection is used:

(ii) Install a write protection device.

(iii) Boot system with the examiner's controlled operating system.

(iv) If software writes protection is used.

(v) Boot system with the examiner-controlled operating system.

(vi) Activate write protection.

(vii) Investigate the geometry of any storage devices to ensure that all space is accounted for, including host-protected data areas (e.g.,

non-host specific data such as the partition table matches the physical geometry of the drive).

(viii) Capture the electronic serial number of the drive and other user-accessible, host-specific data. Acquire the subject evidence to the examiner's storage device using the appropriate software and hardware tools, such as.

(ix) Stand-alone duplication software.

(x) Forensic analysis software suite.

(xi) Dedicated hardware devices.

(xii) Verify successful acquisition by comparing known values of the original and the copy or by doing a sector-by-sector comparison of the original to the copy.

7. Evidence Examination

7.1 Principle

General forensic principles apply when examining digital evidence. Different types of cases and media may require different methods of examination. Persons conducting an examination of digital evidence should be trained for this purpose.

7.2 Procedure

Conduct the examination on data that have been acquired using accepted forensic procedures. Whenever possible, the examination should not be conducted on original evidence. When conducting evidence examination, consider using the following steps:

7.2.1 Preparation (Step 1)

Prepare working directory/directories on separate media to which evidentiary files and data can be recovered and/or extracted.

7.2.2 Extraction (Step 2)

Discussed below are two different types of extraction, physical and logical. The physical extraction phase identifies and recovers data across the entire physical drive without regard to file system. The logical extraction phase identifies and recovers files and data based on the installed operating system(s), file system(s), and/or application(s).

(a) **Physical extraction**

During this stage the extraction of the data from the drive occurs at the physical level regardless of file systems present on the drive. This may include the following methods: keyword searching, file carving, and extraction of the partition table and unused space on the physical drive.

(i) Performing a keyword search across the physical drive may be useful as it allows the examiner to extract data that may not be accounted for by the operating system and file system.

(ii) File carving utilities processed across the physical drive may assist in recovering and extracting useable files and data that may not be accounted for by the operating system and file system.

(iii) Examining the partition structure may identify the file systems present and determine if the entire physical size of the hard drive is accounted for.

(b) **Logical extraction**

During this stage the extraction of the data from the drive is based on the file system(s) present on the drive and may include data from such areas as active files, deleted files, file slack, and unallocated file space. Steps may include:

Extraction of the file system information to reveal characteristics such as directory structure, file attributes, file names, date and time stamps, file size, and file location.

(i) Data reduction to identify and eliminate known files through the comparison of calculated hash values to authenticated hash values.

(ii) Extraction of files pertinent to the examination. Methods to accomplish this may be based on file name and extension, file header, file content, and location on the drive.

(iii) Recovery of deleted files.

(iv) Extraction of password-protected, encrypted, and compressed data.

(v) Extraction of file slack.

(vi) Extraction of the unallocated space.

7.2.3 Analysis of extracted data (Step 3)

Analysis is the process of interpreting the extracted data to determine their significance to the case. Some examples of analysis that may be performed include timeframe, data hiding, application and file, and ownership and possession. Analysis may require a review of the request for service, legal authority for the search of the digital evidence, investigative leads, and/or analytical leads.

(a) **Timeframe analysis**

Timeframe analysis can be useful in determining when events occurred on a computer system, which can be used as a part of associating usage of the computer to an individual(s) at the time the events occurred. Two methods that can be used are:

(i) Reviewing the time and date stamps contained in the file system metadata (e.g., last modified, last accessed, created, change of status) to link files of interest to the timeframes relevant to the investigation. An example of this analysis would be using the last modified date and time to establish when the contents of a file were last changed.

(ii) Reviewing system and application logs that may be present. These may include error logs, installation logs, connection logs, security logs, etc. For example, examination of a security log may indicate when a user name/password combination was used to log into a system.

Note: Take into consideration any differences in the individual's computer date and time as reported in the BIOS.

(b) **Data hiding analysis**

Data can be concealed on a computer system. Data hiding analysis can be useful in detecting and recovering such data and may indicate knowledge, ownership, or intent. Methods that can be used include:

(i) correlating the file headers to the corresponding file extensions to identify any mismatches. Presence of mismatches may indicate that the user intentionally hid data.

(ii) gaining access to all password-protected, encrypted, and compressed files, which may indicate an attempt to conceal

the data from unauthorized users. A password itself may be as relevant as the contents of the file.

(iii) gaining access to a host-protected area (HPA). The presence of user-created data in an HPA may indicate an attempt to conceal data.

(c) **Application and file analysis**

Many programs and files identified may contain information relevant to the investigation and provide insight into the capability of the system and the knowledge of the user. Results of this analysis may indicate additional steps that need to be taken in the extraction and analysis processes. Some examples include:

(i) reviewing file names for relevance and patterns.

(ii) examining file content.

(iii) identifying the number and type of operating system(s).

(iv) correlating the files to the installed applications.

(v) considering relationships between files. For example, correlating Internet history to cache files and e-mail files to e-mail attachments.

(vi) identifying unknown file types to determine their value to the investigation.

(vii) examining the users' default storage location(s) for applications and the file structure of the drive to determine if files have been stored in their default or an alternate location(s).

(viii) examining user-configuration settings.

(ix) analyzing file metadata, the content of the user-created file containing data additional to that presented to the user, typically viewed through the application that created it. For example, files created with word processing applications may include authorship, time last edited, number of times edited, and where they were printed or saved.

d. **Ownership and possession**

In some instances, it may be essential to identify the individual(s) who created, modified, or accessed a file. It may also be important to determine ownership and knowledgeable possession of the questioned data. Elements of knowledgeable possession may be based on the analysis described above, including one or more of the following factors.

(i) Placing the subject at the computer at a particular date and time may help determine ownership and possession (timeframe analysis).

(ii) Files of interest may be located in non-default locations (e.g., user-created directory named "child porn") (application and file analysis).

(iii) The file name itself may be of evidentiary value and also may indicate the contents of the file (application and file analysis).

(iv) Hidden data may indicate a deliberate attempt to avoid detection (hidden data analysis).

(v) If the passwords needed to gain access to encrypted and password-protected files are recovered, the passwords themselves may indicate possession or ownership (hidden data analysis).

(vi) Contents of a file may indicate ownership or possession by containing information specific to a user (application and file analysis).

7.2.4 **Conclusion (Step 4)**

In and of themselves, results obtained from any one of these steps may not be sufficient to draw a conclusion. When viewed as a whole, however, associations between individual results may provide a more complete picture. As a final step in the examination process, be sure to consider the results of the extraction and analysis in their entirety.

8. Documentation and Reporting

8.1 Principle

The examiner is responsible for completely and accurately reporting his or her findings and the results of the analysis of the digital evidence examination.

Documentation is an ongoing process throughout the examination. It is important to accurately record the steps taken during the digital evidence examination.

8.2 **Procedure**

All documentation should be complete, accurate, and comprehensive. The resulting report should be written for the intended audience.

8.3 **Examiner's notes**

Documentation should be contemporaneous with the examination, and retention of notes should be consistent with departmental policies. The following is a list of general considerations that may assist the examiner throughout the documentation process.

(i) Take notes when consulting with the case investigator and/or prosecutor.

(ii) Maintain a copy of the search authority with the case notes.

(iii) Maintain the initial request for assistance with the case file.

(iv) Maintain a copy of chain of custody documentation.

(v) Take notes detailed enough to allow complete duplication of actions.

(vi) Include in the notes dates, times, and descriptions and results of actions taken.

(vii) Document irregularities encountered and any actions taken regarding the irregularities during the examination.

(viii) Include additional information, such as network topology, list of authorized users, user agreements, and/or passwords.

(ix) Document changes made to the system or network by or at the direction of Government / Public sector organizations or the examiner.

(x) Document the operating system and relevant software version and current, installed patches.

(xi) Document information obtained at the scene regarding remote storage, remote user access, and offsite backups.

During the course of an examination, information of evidentiary value may be found that is beyond the scope of the current legal authority. Document this information and bring it to the attention of the Director Cybercrime Wing because the information may be needed to obtain additional search authorities.

8.4 Examiner's report

This section provides guidance in preparing the report that will be submitted to the investigator, prosecutor, and others. These are general suggestions; departmental policy may dictate report writing specifics, such as its order and contents. The report may include:

(i) Identity of the reporting agency.

(ii) Case identifier or submission number.

(iii) Case investigator.

(iv) Identity of the submitter.

(v) Date of receipt.

(vi) Date of report.

(vii) Descriptive list of items submitted for examination, including serial number, make, and model.

(viii) Identity and signature of the examiner.

(ix) Brief description of steps taken during examination, such as string searches, graphics image searches, and recovering erased files.

(x) Results/conclusions.

8.5 Summary of findings

This section may consist of a brief summary of the results of the examinations performed on the items submitted for analysis. All findings listed in

the summary should also be contained in the details of findings section of the report.

8.6 Details of findings

This section should describe in greater detail the results of the examinations and may include:

(i) Specific files related to the request.

(ii) Other files, including deleted files that support the findings.

(iii) String searches, keyword searches, and text string searches.

(iv) Internet-related evidence, such as Web site traffic analysis, chat logs, cache files, e-mail, and news group activity.

(v) Graphic image analysis.

(vi) Indicators of ownership, which could include program registration data.

(vii) Data analysis.

(viii) Description of relevant programs on the examined items.

(ix) Techniques used to hide or mask data, such as encryption, steganography, hidden attributes, hidden partitions, and file name anomalies.

8.7 Supporting materials

List supporting materials that are included with the report, such as print outs of particular items of evidence, digital copies of evidence, and chain of custody documentation.

8.8 Glossary

A glossary may be included with the report to assist the reader in understanding any technical terms used. Use a generally accepted source for the definition of the terms and include appropriate references.

DIGITAL EVIDENCE RECEIVING
(FORM-1)

1. Receiving Details

SR #	Laboratory Case File No.			Date & Time of Receiving	
	Name of the Organization from which the equipment is received	Name			
		Address			
		Contact No.			
	Type of evidence to be required by the said organization				

2. Detail of Digital Equipment

SR #	Item No.	Description of the evidence	Model No/Serial No.	Brand/Manufacturer Name

3. Chain of Custody Log

SR #	Exhibit/Seizure Number	Date / Time / Location of transfer	Delivered by	Received by

CHECKLIST FOR ANALYSIS OF DIGITAL DEVICES IN FORENSIC LAB
(FORM -4)

S.No	Task/Operation	Check Box
1.	Physically examine the received electronic/digital media devices in order to identify the significant problems/damaged items.	
2.	Verify the integrity of seized items.	
3.	Tagged all received items like CPU, hard disks, CDs, USBs, etc	
4.	Photograph all received items.	
5.	Fill form "F-31" (Electronic Device Receiving Form).	
6.	Always use write blocker.	
7.	Open/remove the CPU case and Photograph the internal components	
8.	Search for fire flash drives.	
9.	Document all the items along-with serial #/model # and brands name	
10.	Firstly read the requirement(s) of investigation officer/reporting agency.	
11.	Always use physical/bit stream image for forensic analysis/examination.(Hashing)	
12.	Import all bit stream data into the software (FTK, Encase etc)	
13.	Index all imported data	
14.	Carving the data	
15.	Analyze the evidence such that analysis should meet the requirements of investigation officer/reporting agency	
16.	Record/ print the timeline and directory structure of the evidence.	
17.	Perform keyword search	
18.	See recent documents/files	
19.	Search for deleted items	
20.	Visualize the internet history/cookies/email correspondence, etc	
21.	Search in normal files/hidden files/encrypted files, etc.	
22.	Evaluate the file slack and swap files, etc	
23.	Document the computer media analysis report	
24.	Verify your findings in comparison with the requirements provided by the IO/reporting agency	
25.	Stored the item / evidence securely in lock	
26.	Prepare and signed the forensic report for further case processing.	

SCHEDULE VII
[*See rule 17(5)*]

Terms of Reference of Joint Investigation Team

Introduction

One aspect of close coordination between FIA, police and other intelligence agencies is the referral of cases to Joint Investigation Team, and the related sharing of investigative reports, forensic analysis and sensitive case information. Close collaboration in criminal cases are signs of trust and partnership between Government / Public sector organizations and intelligence agencies.

The government on its own or at the request of the investigation agency, may constitute one or more joint investigation teams, comprising of representatives from cyber-crimes wing, provincial police and intelligence agencies. The joint investigation team so constituted by the government shall jointly work to investigate offences under the Act. The team shall work under clearly defined Terms of Reference covering its essential elements and parameters.

Purpose of Terms of Reference

The purpose of these terms of reference is to clarify the composition, responsibilities, duties, and limitations of any joint investigative team appointed by the government, for the purpose of conducting a joint investigation.

Mandate of Joint Investigation Team

The mandate of the Joint Investigation Team is to plan and conduct a joint investigation into cases under the Act.

Appointment and Composition of Investigation Team

Upon registration of a case under above referred sections, the concerned Cybercrime Circle in-charge will refer the case to the Director General (DG) FIA through the Office of Additional Director General for Cyber Crimes. Depending on the seriousness of the offence, DG FIA will forward the case to the Ministry of Interior for the constitution of Joint Investigation Team. Upon constitution of Joint Investigation Team, the FIA Cybercrime Wing will take the overall "lead" for the completion of investigation and its submission before the competent Court.

In the case of a joint investigation, the Head of the Cybercrime Wing, the Head of local Police and the Heads of the respective intelligence agencies will be responsible for nominating the Joint Investigation Team members. To ensure objectivity and accountability, the investigation team will be comprised of a minimum of three persons, one lead investigator and two supporting investigators as under:

(i) Officer(s) of the Cybercrime Wing not below the rank of BS-19;

(ii) Officer(s) of the intelligence agency(s) not below the rank of BS-18; and

(iii) Officer (s) of provincial/local police not below the rank of BS-18.

Responsibilities of the Joint Investigation Team

The appointed Joint Investigation Team is responsible for the following:

(i) Developing a clear and comprehensive investigation plan.

(ii) Conducting the investigation in accordance with the Act and Prevention of Electronic Crimes Investigation Rules, 2018.

(iii) Evaluating and making recommendations on the needs of the victim and witnesses.

(iv) Reporting the conclusions of the investigation and the investigation process to the Head of the Cybercrime Wing, the Heads of participating intelligence agencies and police.

(v) Producing an accurate and comprehensive report of the investigation.

The investigative responsibilities of the Joint Investigation Team shall apply to the specific case only. They do not apply to other offences unrelated to the case under investigation. Furthermore, the Joint Investigation Team is responsible for ensuring that the scope of the investigation remains restricted to the allegation and does not involve queries, interviews, document collection, or any other investigative action which seeks information unrelated to the allegation.

Responsibilities of lead investigator

The lead investigator's responsibilities are to oversee the investigation, take strategic decisions and create the conditions for investigators to do their work. This includes:

(i) making the key decisions about the direction of the investigation;

(ii) liaising with external institutional stakeholders, such as national authorities and other agencies;

(iii) managing the relationship between the investigation team and the participating agencies; and

(iv) preparing the final investigation report.

Responsibilities of investigators

Investigators are responsible for the day-to-day conduct of the investigation, as defined by TORs. Normally, their responsibilities include:

(i) developing the investigation plan;

(ii) assessing and making recommendations on safety and confidentiality;

(iii) securing evidence;

(iv) gathering evidence;

(v) assisting the lead investigator in preparation of the final report; and

(vi) making a finding on the evidence

Basic qualifications of JIT members

At minimum, JIT members must be:

(i) **professional** – exercise sound judgment and exhibit skill;

(ii) **responsible** – trustworthy, dependable and personally accountable for the decisions they take throughout the investigation;

(iii) **qualified** – have undergone investigation training, and are experienced in investigations;

(iv) **independent**– have no material, personal or professional interest in the outcome of the complaint and no personal or professional connection with any witnesses (especially the complainant and accused of the investigation).

Persons responsible for the investigation must maintain objectivity, impartiality and fairness throughout the investigative process and conduct their activities competently and with the highest levels of integrity.

Witness preferences

Keeping in view the nature of case, the investigation team members must be specialist in their field. It is always best to focus on the right skill set over witness preferences when composing the team as there is no rule that each member of the investigation team must meet the preferences of all witnesses involved. Nevertheless, the investigators should try to make sure that the survivor and any vulnerable witnesses feel comfortable with whoever is interviewing them.

Interpreters and translators

In some cases, interpretation and translation during interviews will be necessary. In such cases, the Joint Investigation Team will take measures to

ensure that qualified and experienced interpreters and translators are made available to the witness or survivor. Ideally, investigators will speak the language of most of the potential witnesses. If this is not possible, they should choose an interpreter who, like them, is competent, discreet, independent and appropriate. In addition, the interpreter must understand the nuances of witnesses' language. Moreover, interpreters and translators must sign an oath of confidentiality and should be relied on to maintain that agreement. Interpreters must be instructed to interpret directly what witnesses say without comment or inference.

Other experts

Sometimes, managers should consider taking expert advice or assistance from outsiders. These may include computer specialists, lawyers with in-country legal expertise and specialists in interviewing children or people with disabilities.

Confidentiality

Confidentiality during the investigation process is critically important. The complainant, the witnesses, the accused, and the investigators themselves can be put in danger as a result of the investigation taking place. Therefore, the Joint Investigation Team will define those persons who will be privy to any information to surface throughout the course of investigation and ensure that the victim and other witnesses are informed of who will be made aware of the investigation process and conclusions.

The joint investigation team members will keep all information related to the investigation in the strictest confidence and each investigator agrees that any information or evidence to surface during the investigation will be shared only with the Cybercrime Wing and the relevant Heads of police and intelligence agencies.

SCHEDULE VII

[*See rules 19(1) and 19(2)*]

REPORT TO THE PARLIAMENT

(Section 53 of the Prevention of Electronic Crimes Act, 2016)

Executive Summary:

(Brief account of salient features of the Cybercrime Wing's activities from Jan – Jun/July –Dec)

(FORM-1)

Categorization of Cases																					
Cyber Crime Main Category	Unauthorized Access to System/ Data			Critical Infrastructure / Cyber Terrorism						Hate Speech	Electronic Fraud/ Forgery			Making, obtaining device used in offense		Identity theft		Sexual Exploitation and Abuse			Total
PECA Sections	3	4	5	6	7	8	9	10	12	11	13	14	18	19	15	16	17	20	21	22	
January																					
February																					
March																					
April																					
May																					
June																					
July																					
August																					
September																					
October																					
November																					
December																					
Total																					

(FORM-2)

Complaints/Enquiries/FIRs								
Months	Number of Complaints Received	Number of Enquiries Registered	Number of FIR Registered	Search and Seize Warrant Obtained	Accused Arrested	Cases Challaned	Under Trial	Cases Decided
								Acquittals / Convicted
January								
February								
March								
April								
May								
June								
July								
August								
September								
October								

November									
December									
Total									

[F. No. 3-18/2016-Legal.]

SALMAN GHANI,
Deputy Secretary,

PRINTED BY THE MANAGER, PRINTING CORPORATION OF PAKISTAN PRESS, ISLAMABAD.
PUBLISHED BY THE DEPUTY CONTROLLER, STATIONERY AND FORMS, UNIVERSITY ROAD, KARACHI.