



READING MATERIAL

**Prevention of Electronic Crimes Act, 2016
&
Prevention of Electronic Crimes Investigation Rules, 2018
&
FIA Act, 1974
&
FIA Rules, 1975
FIA (Inquiries & Investigation) Rules, 2002**

Developed by

Mr. Nizamuddin
Librarian

Assisted by
Mr. Raheel Zaheer
Library Attendant

SINDH JUDICIAL ACADEMY, KARACHI

Title:

Prevention of Electronic Crime Act, 2016 and Prevention of Electronic Crime Investigation Rules, 2018 and FIA Act, 1974 and FIA Rules, 1975 and FIA (Inquiries and Investigation) Rules, 2002

Amendment up to date :- (Act. No XXXVII of 2023)

(Date of Amendment- 30thAug-2023)

Compiled & Proof Reading by:

Mr. Nizam-ud-din (Librarian)

Assisted by:

Mr. Raheel Zaheer (Library Attendant)

Year of Publication:

2023

All rights reserved by the Sindh Judicial Academy, Karachi



The Prevention of Electronic Crimes Act, 2016

CONTENTS

CHAPTER I

PRELIMINARY

1. Short title, extent, application and commencement.....	9
2. Definitions.....	9

CHAPTER II

OFFENCES AND PUNISHMENTS

3. Unauthorized access to information system or data	13
4. Unauthorized copying or transmission of data	13
5. Interference with information system or data.....	13
6. Unauthorized access to critical infrastructure information system or data.....	13
7. Unauthorized copying or transmission of critical infrastructure data	14
8. Interference with critical infrastructure information system or data	14
9. Glorification of an offence	14
10. Cyber terrorism.....	14
11. Hate speech	14
12. Recruitment, funding and planning of terrorism	14
13. Electronic forgery.....	14
14. Electronic fraud	15
15. Making, obtaining, or supplying device for use in offence	15
16. Unauthorized use of identity information.....	15
17. Unauthorized issuance of SIM cards etc	15
18. Tampering, etc. of communication equipment.....	15
19. Unauthorized interception	16
20. Offences against dignity of a natural person	16
21. Offences against modesty of a natural person and minor.....	16
22. Child pornography.....	17
22A. Online grooming, solicitation and cyber enticement.....	17
22B. Commercial sexual exploitation of children.....	17
22C. Use of information system for kidnapping, abduction or trafficking of minor.....	18
23. Malicious code	18
24. Cyber stalking	18

24A. Cyberbullying[New Amendment]	19
25. Spamming.....	19
26. Spoofing	19
27. Legal recognition of offences committed in relation to information system	19
28. Pakistan Penal Code, 1860 (Act XLV of 1860) to apply	20

CHAPTER III

ESTABLISHMENT OF INVESTIGATION AGENCY AND PROCEDURAL POWERS FOR INVESTIGATION

29. Establishment of investigation agency	20
30. Power and procedure to investigate.....	20
30A. Remand[New Amendment].....	21
30B. Victim and witness protection. [New Amendment]	21
30C. In-camera trial. [New Amendment].....	22
30D Investigation into the child sexual content referred to Pakistan Telecommunication Authority	22
31. Expedited preservation and acquisition of data.....	22
32. Retention of traffic data.....	23
33. Warrant for search or seizure	23
34. Warrant for disclosure of content data	23
35. Powers of an authorized officer.....	24
36. Dealing with seized data or information system	25
37. Unlawful on-line content.....	26
38. Limitation of liability of service providers.....	26
39. Real-time collection and recording of information	27
40. Forensic laboratory.....	28
41. Confidentiality of information.....	28

CHAPTER IV

INTERNATIONAL COOPERATION

42. International cooperation.....	28
------------------------------------	----

CHAPTER - V

PROSECUTION AND TRIAL OF OFFENCES

43. Offences to be compoundable and non-cognizable.....	30
43A. Complaint against cybercrimes against children. [New Amendment]-	30
44. Cognizance and trial of offences	30
45. Order for payment of compensation.....	30
45A. Support mechanism for the victims[New Amendment]	30

46. Appointment of amicus curiae and seeking expert opinion	30
47. Appeal	31

CHAPTER VI PREVENTIVE MEASURES

48. Prevention of electronic crimes	31
49. Computer emergency response teams	31

CHAPTER VII MISCELLANEOUS

50. Relation of the Act with other laws	31
51. Power to make rules	31
52. Removal of difficulties	32
53. Report to Parliament.....	33
54. Amendment of Electronic Transactions Ordinance, 2002 (LI of 2002) and pending proceedings	33
55. Savings of powers	33

PREVENTION OF ELECTRONIC CRIMES INVESTIGATION RULES, 2018

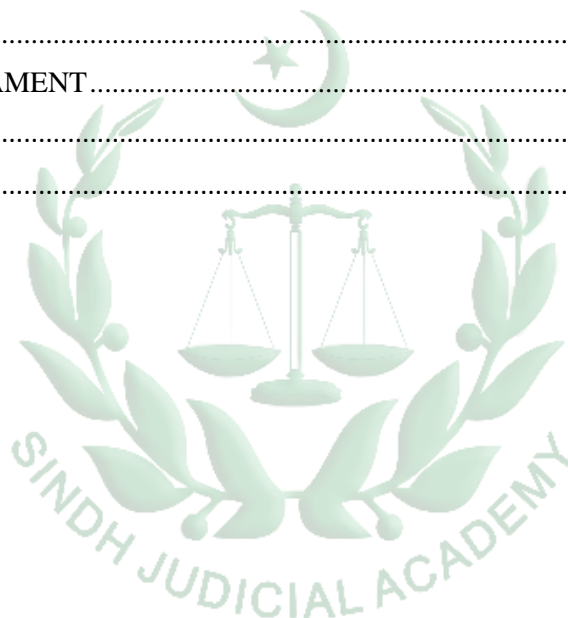
1. Short title and commencement	34
2. Definitions	34
3. Investigation agency	35
4. Cybercrime Wing	35
5. Powers, functions and responsibilities of cybercrime officers	36
6. Cybercrime complaint registration	36
7. Investigation and case procedure.....	36
8. Search and seizure	37
9. Investigation of offences against modesty and dignity of natural persons	37
10. Transfer of investigation	37
11. Forensic capability	37
12. Expert opinion	38
13. Re-examination of digital forensic	38
14. Standard operating procedures and guidelines	38
15. Mandatory training courses	38
16. Appointment, promotions and transfer.....	39
17. Joint investigation team.....	39
18. Cooperation with foreign government, international organization or agency	39

19. Report to the Parliament.....	39
20. Principles and values of investigation	40
SCHEDULE I.....	40
<i>[See rules 4(1) and 16(1)]</i>	<i>40</i>
JOB DESCRIPTION AND QUALIFICATIONS	40
1. ADDITIONAL DIRECTOR GENERAL (BPS-21)	40
Job description	40
2. DIRECTOR (BPS-20).....	41
Job description.....	41
3. ADDITIONAL DIRECTOR OPERATIONS/CRIMES (BPS-19)	41
Job description.....	41
4. DEPUTY DIRECTOR INVESTIGATION/CRIME (BPS-18).....	42
Job description.....	42
5. DEPUTY DIRECTOR ADMIN (BS-18).....	43
Job description.....	43
6. DEPUTY DIRECTOR FORENSICS BS-18	44
Job description.....	44
7. DEPUTY DIRECTOR RESEARCH (BS-18).....	44
Job description.....	44
8. DEPUTY DIRECTOR NETWORK SECURITY (BS-18)	45
Job description.....	45
9. DEPUTY DIRECTOR SOFTWARE (BS-18).....	45
Job description.....	45
10. DEPUTY DIRECTOR DATABASE (BS-18)	46
Job description.....	46
11. DEPUTY DIRECTOR LEGAL (BS-18)	46
Job description.....	46
12. ASSISTANT LEGAL ADVISOR (BS-17).....	47
Job description.....	47
13. ASSISTANT DIRECTOR CYBER CRIME INVESTIGATION (BS-17).....	47
Job description.....	47
14. ASSISTANT DIRECTOR ADMIN (BS-17)	48
Job description.....	48
15. ASSISTANT DIRECTOR LOGISTIC (BS-17)	48
Job description.....	48

16. ASSISTANT DIRECTOR, STRESS COUNSELOR (BS-17).....	49
Job description.....	49
17. ASSISTANT DIRECTOR HARDWARE (BS-17).....	49
Job description.....	49
18. ASSISTANT DIRECTOR ACCOUNTS (BS-17)	50
Job description.....	50
19. ASSISTANT DATABASE ADMINISTRATOR (BS-17)	50
Job description.....	50
20. ASSISTANT DIRECTOR NETWORK (BS-17).....	51
Job description.....	51
21. ASSISTANT DIRECTOR/IN-CHARGE HELPDESK (BS-17)	51
Job description.....	51
22. VICTIM AND WITNESS SUPPORT OFFICER (BS-17)	52
Job description.....	52
23. ASSISTANT DIRECTOR FORENSIC (BS-17)	52
Job description.....	52
24. INSPECTOR - CYBER CRIME INVESTIGATOR (BS-16).....	53
Job description.....	53
25. CYBER CRIME ANALYST (BS-16).....	54
Job description.....	54
26. OFFICE SUPERINTENDENT (BS -16)	54
Job description.....	54
27. DATA ENTRY OPERATOR (BS-14).....	54
Job description.....	54
28. TECHNICAL ASSISTANT (BS -14).....	55
Job description.....	55
29. SUB-INSPECTOR - CYBERCRIME INVESTIGATOR (BS-14).....	55
Job description.....	55
30. ASSISTANT (BS-14).....	56
Job description.....	56
31. UDC (BS-11).....	56
Job description.....	56
32. ASSISTANT SUB-INSPECTOR (BS-09).....	56
Job description.....	56
33. LDC (BS-09)	57

Job description.....	57
34. HEAD CONSTABLE (BS-07)	57
Job description.....	57
35. CONSTABLE (BS-05).....	58
Job description.....	58
36. DISPATCHER (BS-05)	58
Job description.....	58
37. DRIVER CONSTABLE (BS-05).....	58
Job description.....	58
38. ELECTRICIAN (BPS-05).....	59
Job description.....	59
39. NAIB QASID (BS-02)	59
Job description.....	59
40. SWEEPER (BS-01)	59
Job description.....	59
SCHEDULE II	59
<i>[See rules 4(7) and 4(11)]</i>	59
Organizational Structure of Cybercrime Wing.....	59
Annex-A	60
Annex-B	60
Cybercrime Headquarters.....	60
Annex-C	61
Cybercrimes Zonal Office	61
Annex-D	61
Cybercrimes Reporting Center	61
Annex-E	62
Digital Forensics Lab	62
SCHEDULE III	62
CYBERCRIME REPORTING CENTERS.....	62
SCHEDULE IV	63
Annex - A	63
INVESTIGATION WORK PLAN	63
Annex - B	64
INVESTIGATION REPORT STRUCTURE.....	64
SCHEDULE V	65

SEIZURE MEMO	65
(FORM - 1).....	65
CHAIN OF CUSTODY	66
(FORM - 2).....	66
SCHEDULE VI.....	66
DIGITAL EVIDENCE RECEIVING	76
(FORM-1).....	76
CHECKLIST FOR ANALYSIS OF DIGITAL DEVICES	77
IN FORENSIC LAB	77
(FORM-4).....	77
SCHEDULE VII	78
SCHEDULE VII	81
<i>[See rules 19(1) and 19(2)]</i>	81
REPORT TO THE PARLIAMENT	81
(FORM-1).....	81
(FORM-2).....	82



The Prevention of Electronic Crimes Act, 2016

ACT NO. XL OF 2016

[19th August, 2016]

An Act to make provisions for prevention of electronic crimes

WHEREAS it is expedient to prevent unauthorized acts with respect to information systems and provide for related offences as well as mechanisms for their investigation, prosecution, trial and international cooperation with respect thereof and for matters connected therewith or ancillary thereto;

It is hereby enacted as follows: ---

CHAPTER I PRELIMINARY

1. Short title, extent, application and commencement. — (1) This Act may be called the Prevention of Electronic Crimes Act, 2016.

(2) It extends to the whole of Pakistan.

(3) It shall apply to every citizen of Pakistan wherever he may be and also to every other person for the time being in Pakistan.

(4) It shall also apply to any act committed outside Pakistan by any person if the act constitutes an offence under this Act and affects a person, property, information system or data located in Pakistan.

(5) It shall come into force at once.

2. Definitions. — (1) In this Act, unless there is anything repugnant in the subject or context,

(i) “act” includes, ---

(a) a series of acts or omissions contrary to the provisions of this Act; or

(b) causing an act to be done by a person either directly or through an automated information system or automated mechanism or self-executing, adaptive or autonomous device and whether having temporary or permanent impact;

(ii) “access to data” means gaining control or ability to use, copy, modify or delete any data held in or generated by any device or information system;

(iii) “access to information system” means gaining control or ability to use any part or whole of an information system whether or not through infringing any security measure;

(iv) “Authority” means the Pakistan Telecommunication Authority established under the Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996);

(v) “authorization” means authorization by law or by the person empowered to make such authorization under the law:---

Provided that where an information system or data is available for open access by the general public, access to or transmission of such information system or data shall be deemed to be authorized for the purposes of this Act;

(vi) “authorized officer” means an officer of the investigation agency authorized to perform any function on behalf of the investigation agency by or under this Act;

¹(via) "child" means a person below the age of eighteen years;"

²(vib) "child sexual abuse content" means the representation, by whatever means, of a child engaged in real or simulated sexually explicit conduct or representation of the sexual parts of a child for primarily sexual purposes;"

(vii) “Code” means the Code of Criminal Procedure, 1898 (Act V of 1898);

³(viia) "complainant" means any person who makes complaints of any offence under this Act and includes a victim or an individual having substantial reasons to believe the offence is being committed or likely to be committed and any authority referring the complaint for investigation;"

(viii) “content data” means any representation of fact, information or concept for processing in an information system including source code or a program suitable to cause an information system to perform a function;

(ix) “Court” means the Court of competent jurisdiction designated under this Act;

(x) “critical infrastructure” means critical elements of infrastructure namely assets, facilities, systems, networks or processes the loss or compromise of which could result in, ---

(a) major detrimental impact on the availability, integrity or delivery of essential services including those services, whose integrity, if compromised, could result in significant loss of life or casualties, taking into account significant economic or social impacts; or

(b) significant impact on national security, national defense, or the functioning of the state:

Provided that the Government may designate any private or Government infrastructure in accordance with the objectives of sub-paragraphs (i) and (ii) above, as critical infrastructure as may be prescribed under this Act;

¹ Inserted by vide S.2 of Act. No XXXVII of 2023.

² Inserted by vide S.2 of Act. No XXXVII of 2023.

³ Inserted by vide S.2 of Act. No XXXVII of 2023.

(xi) “critical infrastructure information system or data” means an information system, program or data that supports or performs a function with respect to a critical infrastructure;

(xii) “damage to an information system” means any unauthorized change in the ordinary working of an information system that impairs its performance, access, output or change in location whether temporary or permanent and with or without causing any change in the system;

(xiii) “data” includes content data and traffic data;

(xiv) “data damage” means alteration, deletion, deterioration, erasure, relocation, suppression of data or making data temporarily or permanently unavailable;

(xv) “device” includes,---

(a) physical device or article;

(b) any electronic or virtual tool that is not in physical form;

(c) a password, access code or similar data, in electronic or other form, by which the whole or any part of an information system is capable of being accessed; or

(d) automated, self-executing, adaptive or autonomous devices, programs or information systems;

(xvi) “dishonest intention” means intention to cause injury, wrongful gain or wrongful loss or harm to any person or to create hatred or incitement to violence;

(xvii) “electronic” includes electrical, digital, magnetic, optical, biometric, electrochemical, electromechanical, wireless or electromagnetic technology;

(xviii) “identity information” means an information which may authenticate or identify an individual or an information system and enable access to any data or information system;

(xix) “information” includes text, message, data, voice, sound, database, video, signals, software, computer programmes, any forms of intelligence as defined under the Pakistan Telecommunication (Reorganization) Act, 1996 (XVII of 1996) and codes including object code and source code;

(xx) “information system” means an electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing any information;

(xxi) “integrity” means, in relation to an electronic document, electronic signature or advanced electronic signature, the electronic document, electronic signature or advanced electronic signature that has not been tampered with, altered or modified since a particular point in time;

(xxii) “interference with information system or data” means and includes an unauthorized act in relation to an information system or data that may disturb its normal working or form with or without causing any actual damage to such system or data;

(xxiii) “investigation agency” means the law enforcement agency established by or designated under this Act;

(xxiv) “minor” means, notwithstanding anything contained in any other law, any person who has not completed the age of eighteen years;

(xxv) “offence” means an offence punishable under this Act except when committed by a person under ten years of age or by a person above ten years of age and under fourteen years of age, who has not attained sufficient maturity of understanding to judge the nature and consequences of his conduct on that occasion;

(xxvi) “rules” means rules made under this Act;

(xxvii) “seize” with respect to an information system or data includes taking possession of such system or data or making and retaining a copy of the data;

⁴(xxviii) "sexually explicit conduct" means actual or simulated-sexual intercourse, including genital-genital, oral-genital, anal- genital, or oral-anal, whether between persons of the same or opposite sex; or

(a) bestiality; or

(b) masturbation; or

(c) sadistic or masochistic abuse; or

(d) lascivious exhibition of the anus, genitals, or pubic area of any person.", and

(iv) after clause (xxviii), the following new clause shall be inserted, namely:-

(xxviii) “service provider” includes a person who,---

⁵(xxviiiia) "sexual abuse of a minor" shall have the same meaning given to "sexual abuse" in section 377A of the Pakistan Penal Code (Act XLV of 1860);

(a) acts as a service provider in relation to sending, receiving, storing, processing or distribution of any electronic communication or the provision of other services in relation to electronic communication through an information system;

⁴New Clauses Inserted by Fed. Act. No XXXVII of 2023.

⁵ New Clause Inserted by S.2 of Fed Act. No XXXVII of 2023.

(b) owns, possesses, operates, manages or controls a public switched network or provides telecommunication services; or

(c) processes or stores data on behalf of such electronic communication service or users of such service;

(xxix) “subscriber information” means any information held in any form by a service provider relating to a subscriber other than traffic data;

(xxx) “traffic data” includes data relating to a communication indicating its origin, destination, route, time, size, duration or type of service;

(xxxi) “unauthorized access” means access to an information system or data which is not available for access by general public, without authorization or in violation of the terms and conditions of the authorization;

(xxxii) “unauthorized interception” shall mean in relation to an information system or data, any interception without authorization; and

(xxxiii) “unsolicited information” means the information which is sent for commercial and marketing purposes against explicit rejection of the recipient and does not include marketing authorized under the law.

(2) Unless the context provides otherwise, any other expression used in this Act or rules made thereunder but not defined in this Act, shall have the same meanings assigned to the expressions in the Pakistan Penal Code, 1860 (Act XLV of 1860), the Code of Criminal Procedure, 1898 (Act V of 1898) and the Qanoon-e-Shahadat, 1984 (P.O.No.X of 1984), as the case may be.

CHAPTER II

OFFENCES AND PUNISHMENTS

3. Unauthorized access to information system or data.— Whoever with dishonest intention gains unauthorized access to any information system or data shall be punished with imprisonment for a term which may extend to three months or with fine which may extend to fifty thousand rupees or with both.

4. Unauthorized copying or transmission of data.— Whoever with dishonest intention and without authorization copies or otherwise transmits or causes to be transmitted any data shall be punished with imprisonment for a term which may extend to six months, or with fine which may extend to one hundred thousand rupees or with both.

5. Interference with information system or data.— Whoever with dishonest intention interferes with or damages or causes to be interfered with or damages any part or whole of an information system or data shall be punished with imprisonment which may extend to two years or with fine which may extend to five hundred thousand rupees or with both.

6. Unauthorized access to critical infrastructure information system or data.— Whoever with dishonest intention gains unauthorized access to any critical infrastructure

information system or data shall be punished with imprisonment which may extend to three years or with fine which may extend to one million rupees or with both.

7. Unauthorized copying or transmission of critical infrastructure data.— Whoever with dishonest intention and without authorization copies or otherwise transmits or causes to be transmitted any critical infrastructure data shall be punished with imprisonment for a term which may extend to five years, or with fine which may extend to five million rupees or with both.

8. Interference with critical infrastructure information system or data.— Whoever with dishonest intention interferes with or damages, or causes to be interfered with or damaged, any part or whole of a critical information system, or data, shall be punished with imprisonment which may extend to seven years or with fine which may extend to ten million rupees or with both.

9. Glorification of an offence.— (1) Whoever prepares or disseminates information, through any information system or device, with the intent to glorify an offence relating to terrorism, or any person convicted of a crime relating to terrorism, or activities of proscribed organizations or individuals or groups shall be punished with imprisonment for a term which may extend to seven years or with fine which may extend to ten million rupees or with both.

Explanation.— For the purposes of this section “glorification” includes depiction of any form of praise or celebration in a desirable manner.

10. Cyber terrorism.— Whoever commits or threatens to commit any of the offences under sections 6, 7, 8 or 9, where the commission or threat is with the intent to,---

(a) coerce, intimidate, create a sense of fear, panic or insecurity in the Government or the public or a section of the public or community or sect or create a sense of fear or insecurity in society; or

(b) advance inter-faith, sectarian or ethnic hatred; or

(c) advance the objectives of organizations or individuals or groups proscribed under the law, shall be punished with imprisonment of either description for a term which may extend to fourteen years or with fine which may extend to fifty million rupees or with both.

11. Hate speech.—Whoever prepares or disseminates information, through any information system or device, that advances or is likely to advance interfaith, sectarian or racial hatred, shall be punished with imprisonment for a term which may extend to seven years or with fine or with both.

12. Recruitment, funding and planning of terrorism.—Whoever prepares or disseminates information, through any information system or device, that invites or motivates to fund, or recruits people for terrorism or plans for terrorism shall be punished with imprisonment for a term which may extend to seven years or with fine or with both.

13. Electronic forgery.— (1) Whoever interferes with or uses any information system, device or data, with the intent to cause damage or injury to the public or to any person, or to make any illegal claim or title or to cause any person to part with property or to enter into any express or implied contract, or with intent to commit fraud by any input, alteration, deletion, or suppression of data, resulting in

unauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of the fact that the data is directly readable and intelligible or not, shall be punished with imprisonment of either description for a term which may extend to three years, or with fine which may extend to two hundred and fifty thousand rupees or with both.

(2) Whoever commits offence under sub-section (1) in relation to a critical infrastructure information system or data shall be punished with imprisonment for a term which may extend to seven years or with fine which may extend to five million rupees or with both.

14. Electronic fraud.—Whoever with the intent for wrongful gain interferes with or uses any information system, device or data or induces any person to enter into a relationship or deceives any person, which act or omission is likely to cause damage or harm to that person or any other person shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to ten million rupees or with both.

15. Making, obtaining, or supplying device for use in offence. — Whoever produces, makes, generates, adapts, exports, supplies, offers to supply or imports for use any information system, data or device, with the intent to be used or believing that it is primarily to be used to commit or to assist in the commission of an offence under this Act shall, without prejudice to any other liability that he may incur in this behalf, be punished with imprisonment for a term which may extend to six months or with fine which may extend to fifty thousand rupees or with both.

16. Unauthorized use of identity information.— (1) Whoever obtains, sells, possesses, transmits or uses another person's identity information without authorization shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to five million rupees, or with both.

(2) Any person whose identity information is obtained, sold, possessed, used or transmitted may apply to the Authority for securing, destroying, blocking access or preventing transmission of identity information referred to in sub-section (1) and the Authority on receipt of such application may take such measures as deemed appropriate for securing, destroying or preventing transmission of such identity information.

17. Unauthorized issuance of SIM cards etc.—Whoever sells or otherwise provides subscriber identity module (SIM) card, re-usable identification module (R-IUM) or universal integrated circuit card (UICC) or other module designed for authenticating users to establish connection with the network and to be used in cellular mobile, wireless phone or other digital devices such as tablets, without obtaining and verification of the subscriber's antecedents in the mode and manner for the time being approved by the Authority shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to five hundred thousand rupees or with both.

18. Tampering, etc. of communication equipment.—Whoever unlawfully or without authorization changes, alters, tampers with or re-programs unique device identifier of any communication equipment including a cellular or wireless handset and starts using or marketing such device for transmitting and receiving information shall be punished with imprisonment which may extend to three years or with fine which may extend to one million rupees or with both.

Explanation.—A “unique device identifier” is an electronic equipment identifier which is unique to a communication device.

19. Unauthorized interception.— Whoever with dishonest intention commits unauthorized interception by technical means of,---

(a) any transmission that is not intended to be and is not open to the public, from or within an information system; or

(b) electromagnetic emissions from an information system that are carrying data, shall be punished with imprisonment of either description for a term which may extend to two years or with fine which may extend to five hundred thousand rupees or with both.

20. Offences against dignity of a natural person.— (1) Whoever intentionally and publicly exhibits or displays or transmits any information through any information system, which he knows to be false, and intimidates or harms the reputation or privacy of a natural person, shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to one million rupees or with both:

Provided that nothing under this sub-section shall apply to anything aired by a broadcast media or distribution service licensed under the Pakistan Electronic Media Regulatory Authority Ordinance, 2002 (XIII of 2002).

(2) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-section (1) and the Authority on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.

21. Offences against modesty of a natural person and minor.—(1) Whoever intentionally and publicly exhibits or displays or transmits any information which,---

(a) superimposes a photograph of the face of a natural person over any sexually explicit image or video; or

(b) includes a photograph or a video of a natural person in sexually explicit conduct; or

(c) intimidates a natural person with any sexual act, or any sexually explicit image or video of a natural person; or

(d) cultivates, entices or induces a natural person to engage in a sexually explicit act, through an information system to harm a natural person or his reputation, or to take revenge, or to create hatred or to blackmail, shall be punished with imprisonment for a term which may extend to five years or with fine which may extend to five million rupees or with both.

(2) Whoever commits an offence under sub-section (1) with respect to a minor shall be punished with imprisonment for a term which may extend to seven years and with fine which may extend to five million rupees:---

Provided that in case of a person who has been previously convicted of an offence under sub-section (1) with respect to a minor shall be punished with imprisonment for a term of ten years and with fine.

(3) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-section (1) and the Authority, on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.

22. Child pornography.—(1) Whoever intentionally produces, offers or makes available, distributes or transmits through an information system or procures for himself or for another person or without lawful justification possesses material in an information system, that visually depicts,---

- (a) a minor engaged in sexually explicit conduct;
- (b) a person appearing to be a minor engaged in sexually explicit conduct; or
- (c) realistic images representing a minor engaged in sexually explicit conduct; or
- (d) discloses the identity of the minor,

shall be punished with imprisonment for a term which may extend to ⁶[fourteen years and may extend up to twenty years and with fine which shall not be less than one million rupees"].

(2) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-section (1) and the Authority, on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances, including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.

⁷**22A. Online grooming, solicitation and cyber enticement.**—Whoever intentionally creates or takes steps towards creating a relationship of trust with a minor through the use of an information system or device or any other similar means of communication with the intent to facilitate, solicit or commit sexual abuse of a minor or to share, facilitate or solicit sexual content or produce sexual abuse material with a minor, shall be punished with imprisonment of either description for a term which may extend to ten years and not less than five years with fine which may extend to ten million rupees but not less than five hundred thousand rupees.

22B. Commercial sexual exploitation of children. Subject to section 8. whoever is directly or indirectly involved in the use of an information system or other similar means for the purposes of the sexual exploitation of minors including child prostitution and child sex tourism by payment in money or in kind to the minor or any other person shall be punished with imprisonment of either description for a term which shall not be less than fourteen years and may extend up to twenty years and with fine which shall not be less than one million rupees.

⁶ Punishment Substituted by S.3 of Fed.Act No.XXXVII of 2023.

⁷ New Sections 22A, 22B & 22C inserted by S.4 of Fed.Act No.XXXVII of 2023.

22C. Use of information system for kidnapping, abduction or trafficking of minor—Whoever contacts a minor through the use of an information system or any other similar means directly or indirectly of communication with intent to kidnap, abduct or traffic a minor to commit sexual abuse of a minor or exploitation shall be punished with imprisonment of either description for a term which shall not be less than fourteen years and may extend up to twenty years and with fine which shall not be less than one million rupees."].

23. Malicious code.—Whoever willfully and without authorization writes, offers, makes available, distributes or transmits malicious code through an information system or device, with intent to cause harm to any information system or data resulting in the corruption, destruction, alteration, suppression, theft or loss of the information system or data shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to one million rupees or with both.

Explanation.—For the purpose of this section, the expression “malicious code” includes, a computer program or a hidden function in a program that damages an information system or data or compromises the performance of such system or availability of data or uses it without proper authorization.

24. Cyber stalking.— (1) A person commits the offence of cyber stalking who, with the intent to coerce or intimidate or harass any person, uses information system, information system network, the Internet, website, electronic mail or any other similar means of communication to,---

- (a) follow a person or contacts or attempts to contact such person to foster personal interaction repeatedly despite a clear indication of disinterest by such person;
- (b) monitor the use by a person of the internet, electronic mail, text message or any other form of electronic communication;
- (c) watch or spy upon a person in a manner that results in fear of violence or serious alarm or distress, in the mind of such person; or
- (d) take a photograph or make a video of any person and displays or distributes it without his consent in a manner that harms a person.

(2) Whoever commits the offence specified in sub-section (1) shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to one million rupees or with both:---

Provided that if victim of the cyber stalking under sub-section (1) is a minor the punishment may extend to five years or with fine which may extend to ten million rupees or with both.

(3) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-section (1) and the Authority, on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.

⁸**[24A. Cyberbullying.** (1) A person commits the offence of cyberbullying who, with intent to harass, threaten or target another person posts or sends electronic messages, including pictures or videos by using any social media platform, including chat rooms, blogs or instant messaging.

(2) A minor through his guardian may apply to the Authority for removal, destruction of, or blocking access to such content or communication referred to in sub-section (1).

(3) The Authority, on receipt of application under sub-section (2), shall forthwith pass such orders as deemed appropriate in the circumstances including an order for removal, destruction, preventing transmission of or blocking access to such content and communication.

(4) The Authority shall, before passing an order under sub-section (3), seek report from investigation agency whether or not such content is required for investigation or prosecution purposes.

(5) Whoever commits the offence of child cyberbullying as described in sub-section (1), shall be punished with imprisonment of either description for a term which may extend to five years but shall not be less than one year with a fine of up to five hundred thousand rupees and shall not less than one hundred thousand rupees ".

25. Spamming. — (1) A person commits the offence of spamming, who with intent transmits harmful, fraudulent, misleading, illegal or unsolicited information to any person without permission of the recipient or who causes any information system to show any such information for wrongful gain.

(2) A person including an institution or an organization engaged in direct marketing shall provide the option to the recipient of direct marketing to unsubscribe from such marketing.

(3) Whoever commits the offence of spamming as described in sub-section (1) by transmitting harmful, fraudulent, misleading or illegal information, shall be punished with imprisonment for a term which may extend to three months or with fine of rupees fifty thousand which may extend up to rupees five million or with both.

(4) Whoever commits the offence of spamming as described in sub-section (1) by transmitting unsolicited information, or engages in direct marketing in violation of sub-section (2), for the first time, shall be punished with fine not exceeding fifty thousand rupees, and for every subsequent violation shall be punished with fine not less than fifty thousand rupees that may extend up to one million rupees.

26. Spoofing. — (1) Whoever with dishonest intention establishes a website or sends any information with a counterfeit source intended to be believed by the recipient or visitor of the website, to be an authentic source commits spoofing.

(2) Whoever commits spoofing shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to five hundred thousand rupees or with both.

27. Legal recognition of offences committed in relation to information system. — (1) Notwithstanding anything contained in any other law for the time being in force, an offence under this Act or any other law shall not be denied legal recognition and enforcement for the sole reason of such offence being committed in relation to or through the use of an information system.

⁸ New Section inserted by S.5 of Fed.Act No.XXXVII of 2023.

(2) References to “property” in any law creating an offence in relation to or concerning property, shall include information system and data.

28. Pakistan Penal Code, 1860 (Act XLV of 1860) to apply.—The provisions of the Pakistan Penal Code, 1860 (Act XLV of 1860), to the extent not inconsistent with anything provided in this Act, shall apply to the offences provided in this Act.

CHAPTER III

ESTABLISHMENT OF INVESTIGATION AGENCY AND PROCEDURAL POWERS FOR INVESTIGATION

29. Establishment of investigation agency.— (1) The Federal Government may establish or designate a law enforcement agency as the investigation agency for the purposes of investigation of offences under this Act.

(2) Unless otherwise provided for under this Act, the investigation agency and the authorized officer shall in all matters follow the procedure laid down in the Code to the extent that it is not inconsistent with any provision of this Act.

(3) The investigation agency shall establish its own capacity for forensic analysis of the data or in information systems and the forensic analysis reports generated by the investigation agency shall not be inadmissible in evidence before any court for the sole reason that such reports were generated by the investigation agency.

(4) Notwithstanding provisions of any other law, the Federal Government shall make rules for appointment and promotion in the investigation agency including undertaking of specialized courses in digital forensics, information technology, computer science and other related matters for training of the officers and staff of the investigation agency.

⁹[30. Power and procedure to investigate. (1) In addition to the Federal Investigation Agency, the Police shall be authorized to take cognizance of the offences under this Act. In that case the Police shall be bound to refer the matter relating offence under this Act immediately to the Federal Investigation Agency, for technical opinion and investigation as per its mandate and rules:

Provided that the Federal or Provincial Government, as the case may be, may constitute one or more joint investigation teams comprising of an authorized officer of the investigation agency and any other law enforcement agency for investigation of an offence under this Act and any other law for the time being in force

(2) An investigating officer under this Act shall be an officer or Police not below the rank of Inspector of Police or equivalent or, if the Federal Government or the Provincial Government, as the case may, deems necessary to constitute a Joint Investigation Team it shall be headed by an Investigating Officer not below the rank of BS-18 and other officers of Joint Investigation Team may include equivalent rank from other agencies, as the case may be. The Joint Investigation Team shall comprise five members and for the meeting purposes the quorum shall consists of three members.

⁹ Section 30 substituted by Sec. 6 of Fed.Act No.XXXVII of 2023.

(3) The investigating officer or the Joint Investigation Team, as case may be, shall complete the investigation in respect of cases triable by the court within forty-five working days.

(4) The Court shall, on taking cognizance of a case under this Act, proceed with the trial on weekly basis and shall decide the case within three months, failing which the matter shall be brought, to the notice of the Chief Justice of the High Court concerned for appropriate directions, keeping in view the facts and circumstances of the case.”

¹⁰[**30A. Remand.** (1) Where a person is detained for investigation, the investigating officer, within twenty-four hours of the arrest, excluding the time necessary for the journey from the place of arrest to the Court, shall produce the accused before the Court, and may apply for remand of the accused to police custody, or custody of any other investigating agency joined in the investigation for which the maximum period allowed must not be more than fourteen days at one time:

Provided that, where an accused cannot within twenty four hours be produced before the Court, a temporary order for police custody or custody of any other investigating agency joined in the investigation not exceeding twenty- four hours may be obtained from the nearest Magistrate for the purpose of producing the accused before the Court within that period.

(2) No extension in time of the remand of the accused in police custody or custody of any other investigating agency joined in the investigation shall be allowed, unless it can be shown by the investigating officer, to the satisfaction of the Court that further evidence may be available and the Court is satisfied that no bodily harm has been or will be caused to the accused:

Provided that the total period of such remand shall not in any case exceed thirty days.

03) The Court shall be deemed to be a Magistrate for purposes of sub- section (2)"

30B. Victim and witness protection. (1) A victim and witness protection system shall be established by the Federal and Provincial Governments of Pakistan through rules with features including the following, namely

(i) special security arrangements for witnesses and victims;

(ii) concealment of identity.

(iii) distance recording of testimonies through video-conferencing, audio-video links and by the use of modern devices;

(iv) re-location of victims and witnesses;

(v) provision of reasonable financial assistance;

(vi) compensation to legal heirs of protected victims and witnesses;

¹⁰ New Sections 30A, 30B, 30C & 30D Inserted by S.7 of Fed.Act No.XXXVII of 2023.

(vii) safe-houses, dar-ul-amans etc.; and

(viii) such other measures as may be necessary and ancillary.

(2) Till such time the rules envisaged in sub-section (1) are prescribed, the witness protection system and benefits prescribed under the Witness Protection, Security and Benefit Act, 2017 (XXI of 2017) shall be applicable to both victims and witnesses under this Act, mutatis mutandis.

30C. In-camera trial. (1) The trial of offences against minors shall be conducted in-camera:

Provided that the Court, if it thinks fit, on its own or on an application made by either of parties, allow any particular person to have access to Court proceedings, or be or remain in the Court.

(2) Notwithstanding anything contained in any other law for the time being in force, where any proceedings are held under sub-section (1), the Court may adopt appropriate measures, including holding of the trial through video-link or usage of screens, for the protection of the victims and the witnesses.

(3) Where any proceedings are held under sub-section (1), it shall not be lawful for any person to publish or broadcast any matter or information in relation to any such proceedings, except with the permission of the Court.

30D. Investigation into the child sexual content referred to Pakistan Telecommunication Authority. The Federal Investigation Agency shall acquire the information of the child sexual abuse content referred for blocking and removal to Pakistan Telecommunication Authority and the organizations having data in this regard, for investigation prior to their removal and blocking by said Authority, whether the direct complaint against the said material has been made or not.”

31. Expedited preservation and acquisition of data.— (1) If an authorised officer is satisfied that,---

(a) specific data stored in any information system or by means of an information system is reasonably required for the purposes of a criminal investigation; and

(b) there is a risk or vulnerability that the data may be modified, lost, destroyed or rendered inaccessible, the authorized officer may,

by written notice given to the person in control of the information system, require that person to provide that data or to ensure that the data specified in the notice be preserved and the integrity thereof is maintained for a period not exceeding ninety days as specified in the notice:---

Provided that the authorized officer shall immediately but not later than twenty-four hours bring to the notice of the Court, the fact of acquisition of such data and the Court on receipt of such information may pass such orders as deemed appropriate in the circumstances of the case including issuance of warrants for retention of such data or otherwise.

(2) The period provided in sub-section (1) for preservation of data may be extended by the Court if so deemed necessary upon receipt of an application from the authorized officer in this behalf

32. Retention of traffic data.—(1) A service provider shall, within its existing or required technical capability, retain its specified traffic data for a minimum period of one year or such period as the Authority may notify from time to time and, subject to production of a warrant issued by the Court, provide that data to the investigation agency or the authorized officer whenever so required.

(2) The service providers shall retain the traffic data under sub-section (1) by fulfilling all the requirements of data retention and its originality as provided under sections 5 and 6 of the Electronic Transactions Ordinance, 2002 (LI of 2002).

(3) Any owner of the information system who is not a licensee of the Authority and violates sub-section (1) shall be guilty of an offence punishable, if committed for the first time, with fine which may extend to ten million rupees and upon any subsequent conviction shall be punishable with imprisonment which may extend to six months or with fine or with both:---

Provided that where the violation is committed by a licensee of the Authority, the same shall be deemed to be a violation of the terms and conditions of the licensee and shall be treated as such under the Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996).

33. Warrant for search or seizure.—(1) Upon an application by an authorized officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that there may be in a specified place an information system, data, device or other articles that,---

(a) may reasonably be required for the purpose of a criminal investigation or criminal proceedings which may be material as evidence in proving a specifically identified offence made out under this Act; or

(b) has been acquired by a person as a result of the commission of an offence, the Court may issue a warrant which shall authorize an officer of the investigation agency, with such assistance as may be necessary, to enter the specified place and to search the premises and any information system, data, device or storage medium relevant to the offence identified in the application and access, seize or similarly secure any information system, data, device or other articles relevant to the offence identified in the application.

(2) In circumstances involving an offence under section 10, under which a warrant may be issued but cannot be obtained without the apprehension of destruction, alteration or loss of data, information system, data, device or other articles required for investigation, the authorized officer, who shall be a Gazetted officer of the investigation agency, may enter the specified place and search the premises and any information system, data, device or other articles relevant to the offence and access, seize or similarly secure any information system, data, device or other articles relevant to the offence:---

Provided that the authorized officer shall immediately but not later than twenty-four hours bring to the notice of the Court, the fact of such search or seizure and the Court on receipt of such information may pass such orders as deemed appropriate in the circumstances of the case.

34. Warrant for disclosure of content data.—(1) Upon an application by an authorised officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe

that the content data stored in an information system is reasonably required for the purpose of a criminal investigation or criminal proceedings with respect to an offence made out under this Act, the Court may, after recording reasons, order that the person in control of the data or information system, to provide such data or access to such data to the authorized officer.

(2) The period of a warrant issued under sub-section (1) may be extended beyond seven days if, on application, a Court authorizes an extension for a further period of time as may be specified by the Court.

35. Powers of an authorized officer.— (1) Subject to provisions of this Act, an authorized officer shall have the powers to,---

- (a) have access to and inspect the operation of any specified information system;
- (b) use or cause to be used any specified information system to search any specified data contained in or available to such system;
- (c) obtain and copy only relevant data, use equipment to make copies and obtain an intelligible output from an information system;
- (d) have access to or demand any information in readable and comprehensible format or plain version;
- (e) require any person by whom or on whose behalf, the authorized officer has reasonable cause to believe, any information system has been used to grant access to any data within an information system within the control of such person;
- (f) require any person having charge of or otherwise concerned with the operation of any information system to provide him reasonable technical and other assistance as the authorized officer may require for investigation of an offence under this Act; and
- (g) require any person who is in possession of decryption information of an information system, device or data under investigation to grant him access to such data, device or information system in unencrypted or decrypted intelligible format for the purpose of investigating any such offence:---

Explanation.—Decryption information means information or technology that enables a person to readily retransform or unscramble encrypted data from its unreadable form and from ciphered data to intelligible data.

(2) In exercise of the power of search and seizure of any information system, program or data the authorized officer at all times shall,---

- (a) act with proportionality;
- (b) take all precautions to maintain integrity and secrecy of the information system and data in respect of which a warrant for search or seizure has been issued;
- (c) not disrupt or interfere with the integrity or running and operation of any information system or data that is not the subject of the offences identified in the application for which a warrant for search or seizure has been issued;

(d) avoid disruption to the continued legitimate business operations and the premises subjected to search or seizure under this Act; and

(e) avoid disruption to any information system, program or data not connected with the information system that is not the subject of the offences identified in the application for which a warrant has been issued or is not necessary for the investigation of the specified offence in respect of which a warrant has been issued.

(3) When seizing or securing any data or information system, the authorized officer shall make all efforts to use technical measures to maintain its integrity and chain of custody. The authorized officer shall seize an information system, data, device or articles, in part or in whole, as a last resort only in the event where it is not possible under the circumstances to use such technical measures or where use of such technical measures by themselves shall not be sufficient to maintain the integrity and chain of custody of the data or information system being seized.

(4) Where an authorized officer seizes or secures any data or information system, the authorized officer shall ensure that data or information system while in the possession or in the access of the authorized officer is not released to any other person including competitors or public at large and details including log of any action performed on the information system or data is maintained in a manner prescribed under this Act.

36. Dealing with seized data or information system.— (1) If any data or information system has been seized or secured following a search or seizure under this Act, the authorized officer who undertook the search or seizure shall, at the time of the seizure,---

(a) make a list of what has been seized or rendered inaccessible, with the date and time of seizure; and

(b) give a copy of that list to,---

(i) the occupier of the premises; or

(ii) the owner of the data or information system; or

(iii) the person from whose possession the data or information system has been seized, in a prescribed manner in the presence of two witnesses.

(2) The authorized officer, upon an application of the owner of the data or information system or an authorized agent of the owner and on payment of prescribed costs, shall provide forensic image of the data or information system to the owner or his authorized agent within a time prescribed under this Act.

(3) If the authorized officer has reasons to believe that providing forensic image of the data or information system to the owner under sub-section (2) may prejudice,---

(a) the investigation in connection with which the search was carried out; or

(b) another ongoing investigation; or

(c) any criminal proceedings that are pending or that may be brought in relation to any of those investigations, the authorized officer shall, within seven days of receipt of the

application under sub-section (2), approach the Court for seeking an order not to provide copy of the seized data or information system.

(4) The Court, upon receipt of an application from an authorized officer under sub-section (3), may after recording reasons in writing pass such order as deemed appropriate in the circumstances of the case.

(5) The costs associated with the exercise of rights under this section shall be borne by the person exercising these rights.

37. Unlawful on-line content.— (1) The Authority shall have the power to remove or block or issue directions for removal or blocking of access to an information through any information system if it considers it necessary in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, public order, decency or morality, or in relation to contempt of court or commission of or incitement to an offence under this Act.

(2) The Authority shall, with the approval of the Federal Government, prescribe rules providing for, among other matters, safeguards, transparent process and effective oversight mechanism for exercise of powers under sub-section (1).

(3) Until such rules are prescribed under sub-section (2), the Authority shall exercise its powers under this Act or any other law for the time being in force in accordance with the directions issued by the Federal Government not inconsistent with the provisions of this Act.

(4) Any person aggrieved from any order passed by the Authority under sub-section (1), may file an application with the Authority for review of the order within thirty days from the date of passing of the order.

(5) An appeal against the decision of the Authority in review shall lie before the High Court within thirty days of the order of the Authority in review.

38. Limitation of liability of service providers.— (1) No service provider shall be subject to any civil or criminal liability, unless it is established that the service provider had specific actual knowledge and willful intent to proactively and positively participate, and not merely through omission or failure to act, and thereby facilitated, aided or abetted the use by any person of any information system, service, application, online platform or telecommunication system maintained, controlled or managed by the service provider in connection with a contravention of this Act or rules made thereunder or any other law for the time being in force:---

Provided that the burden to prove that a service provider had specific actual knowledge, and willful intent to proactively and positively participate in any act that gave rise to any civil or criminal liability shall be upon the person alleging such facts and no interim or final orders, or directions shall be issued with respect to a service provider by any investigation agency or Court unless such facts have so been proved and determined:---

Provided further that such allegation and its proof shall clearly identify with specificity the content, material or other aspect with respect to which civil or criminal liability is claimed including but not limited to unique identifiers such as the Account Identification (Account ID), Uniform Resource Locator (URL), Top Level Domain (TLD), Internet Protocol Addresses (IP Addresses), or other unique identifier and clearly state the statutory provision and basis of the claim.

(2) No service provider shall under any circumstance be liable under this Act, rules made thereunder or any other law for maintaining and making available the provision of their service in good faith.

(3) No service provider shall be subject to any civil or criminal liability as a result of informing a subscriber, user or end-users affected by any claim, notice or exercise of any power under this Act, rules made thereunder or any other law:---

Provided that the service provider, for a period not exceeding fourteen days, shall keep confidential and not disclose the existence of any investigation or exercise of any power under this Act when a notice to this effect is served upon it by an authorized officer, which period of confidentiality may be extended beyond fourteen days if, on an application by the authorized officer, the Court authorizes an extension for a further specified period upon being satisfied that reasonable cause for such extension exists.

(4) No service provider shall be liable under this Act, rules made thereunder or any other law for the disclosure of any data or other information that the service provider discloses only to the extent of the provisions of this Act.

(5) No service provider shall be under any obligation to proactively monitor, make inquiries about material or content hosted, cached, routed, relayed, conduit, transmitted or made available by such intermediary or service provider.

39. Real-time collection and recording of information.— (1) If a Court is satisfied on the basis of information furnished by an authorized officer that there are reasonable grounds to believe that the content of any information is reasonably required for the purposes of a specific criminal investigation, the Court may order, with respect to information held by or passing through a service provider, to a designated agency as notified under the Investigation for Fair Trial Act, 2013 (I of 2013) or any other law for the time being in force having capability to collect real time information, to collect or record such information in real-time in coordination with the investigation agency for provision in the prescribed manner:---

Provided that such real-time collection or recording shall not be ordered for a period beyond what is absolutely necessary and in any event for not more than seven days.

(2) Notwithstanding anything contained in any law to the contrary the information so collected under sub-section (1) shall be admissible in evidence.

(3) The period of real-time collection or recording may be extended beyond seven days if, on an application, the Court authorizes an extension for a further specified period.

(4) The Court may also require the designated agency to keep confidential the fact of the execution of any power provided for in this section and any information relating to it.

(5) The application under sub-sections (1) and (2) shall in addition to substantive grounds and reasons also, ---

(a) explain why it is believed that the data sought will be available with the person in control of an information system;

- (b) identify and explain with specificity the type of information likely to be found on such information system;
- (c) identify and explain with specificity the identified offence made out under this Act in respect of which the warrant is sought;
- (d) if authority to seek real-time collection or recording on more than one occasion is needed, explain why and how many further disclosures are needed to achieve the purpose for which the warrant is to be issued;
- (e) specify what measures shall be taken to prepare and ensure that the real-time collection or recording is carried out whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information of any person not part of the investigation;
- (f) explain why the investigation may be frustrated or seriously prejudiced unless the real time collection or recording is permitted; and
- (g) why, to achieve the purpose for which the warrant is being applied, real time collection or recording by the person in control of the information system is necessary.

40. Forensic laboratory.—The Federal Government shall establish or designate a forensic laboratory, independent of the investigation agency, to provide expert opinion before the Court or for the benefit of the investigation agency in relation to electronic evidence collected for purposes of investigation and prosecution of offences under this Act.

41. Confidentiality of information.—Notwithstanding immunity granted under any other law for the time being in force, any person including a service provider while providing services under the terms of lawful contract or otherwise in accordance with the law, or an authorized officer who has secured access to any material or data containing personal information about another person, discloses such material to any other person, except when required by law, without the consent of the person concerned or in breach of lawful contract with the intent to cause or knowing that he is likely to cause harm, wrongful loss or gain to any person or compromise confidentiality of such material or data shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to one million rupees or with both:---

Provided that the burden of proof of any defense taken by an accused service provider or an authorized officer that he was acting in good faith, shall be on such a service provider or the authorized officer, as the case may be.

CHAPTER IV

INTERNATIONAL COOPERATION

42. International cooperation.— (1) The Federal Government may upon receipt of a request, through the designated agency under this Act, extend such cooperation to any foreign government¹¹[including the government of Azad Jammu and Kashmir], 24 x 7 network, any foreign agency or any international organization or agency for the purposes of investigations or proceedings concerning offences related to information systems, electronic communication or data or for the collection of evidence in electronic form relating to an offence or obtaining expeditious preservation and disclosure

¹¹New words Inserted by S.8 of Fed.Act. No. XXXVII of 2023.

of data by means of an information system or real-time collection of data associated with specified communications or interception of data under this Act.

(2) The Federal Government may forward to a foreign government, 24x7 network, any foreign agency or any international agency or organization any information obtained from its own investigations if it considers that the disclosure of such information might assist the other government, agency or organization etc., as the case be, in initiating or carrying out investigations or proceedings concerning any offence under this Act.

(3) The Federal Government shall require the foreign government, 24 x 7 network, any foreign agency or any international organization or agency to keep the information provided confidential and use it strictly for the purposes it is provided.

(4) The Federal Government may, through the designated agency, send and answer requests for mutual assistance the execution of such requests or their transmission to the authorities competent for their execution.

(5) The Federal Government may refuse to accede to any request made by a foreign government, 24 x 7 network, any foreign agency or any international organization or agency, if,---

- (a) it is of the opinion that the request, if granted, would prejudice sovereignty, security, public order or other essential public interest of Pakistan;
- (b) the offence is regarded by the Federal Government as being of a political nature;
- (c) there are substantial grounds for believing that the request for assistance has been made for the purpose of prosecuting a person on account of that person's race, sex, religion, nationality, ethnic origin or political opinions or that that person's position may be prejudiced for any of those reasons;
- (d) the request relates to an offence the prosecution of which in the requesting State may be incompatible with the laws of Pakistan;
- (e) the assistance requested requires the Federal Government to carry out compulsory measures that may be inconsistent with the laws or practices of Pakistan had the offence been the subject of investigation or prosecution under its own jurisdiction; or
- (f) the request concerns an offence which may prejudice an ongoing investigation or trial or rights of its citizens guaranteed under the Constitution.

(6) Where the Federal Government decides to provide the requested cooperation, the relevant requirements and safeguards provided under this Act and rules framed thereunder shall be followed.

(7) The designated agency shall maintain a register of requests received from any foreign government, 24 x 7 network, any foreign agency or any international organization or agency under this Act and action taken thereon.

CHAPTER - V

PROSECUTION AND TRIAL OF OFFENCES

43. Offences to be compoundable and non-cognizable. — (1) All offences under this Act, except the offences under sections 10, 21 and 22 and abetment thereof, shall be non-cognizable, bailable and compoundable: ---

Provided that offences under section 17 shall be cognizable by the investigation agency on a written complaint by the Authority.

(2) Offences under sections 10, 21, ¹²[22, 22A, 22B, 22C] and abetment thereof shall be non-bailable, non-compoundable and cognizable by the investigation agency.

¹³**[43A. Complaint against cybercrimes against children.]**—Complaint against the offences under sections 10, 21, 21A, 21B, 21C, 21D, 21E, 21F and abatement thereof may be lodged with concerned authorities by the complainant as defined under clause (viia) of section 2."..

44. Cognizance and trial of offences.—(1) The Federal Government, in consultation with the Chief Justice of respective High Court, shall designate presiding officers of the Courts to try offences under this Act at such places as deemed necessary.

(2) The Federal Government shall, in consultation with the Chief Justice of respective High Court, arrange for special training of the presiding officers of the Court to be conducted by an entity notified by the Federal Government for training on computer sciences, cyber forensics, electronic transactions and data protection.

(3) Prosecution and trial of an offence under this Act committed by a minor shall be conducted under the Juvenile Justice System Ordinance, 2000 (XXII of 2000).

(4) To the extent not inconsistent with this Act, the procedure laid down under the Code and the Qanoon-e-Shahadat, 1984 (P.O.No.X of 1984), shall be followed.

45. Order for payment of compensation.— (1) The Court may, in addition to award of any punishment including fine under this Act, make an order for payment of compensation to the victim for any damage or loss caused and the compensation so awarded shall be, recoverable as arrears of land revenue:---

Provided that the compensation awarded by the Court shall not prejudice any right to a civil remedy for the recovery of damages beyond the amount of compensation so awarded.

¹⁴**[45A. Support mechanism for the victims.]**—The Government shall develop mechanism for the support of victims in collaboration with other agencies and civil society organizations.

46. Appointment of amicus curiae and seeking expert opinion.—The Court may appoint *amicus curiae* or seek independent expert opinion on any matter connected with a case pending before it.

¹² Expression substituted by S.9 of Fed.Act. No. XXXVII of 2023.

¹³ New Section Inserted by S.10 of Fed.Act. No. XXXVII of 2023.

¹⁴ New Section Inserted by S.11 of Fed.Act. No. XXXVII of 2023.

47. Appeal. — An appeal against the final judgment or order of a Court shall, within thirty days from the date of provision of its certified copy free of cost, lie, ---

(a) to the High Court concerned against such judgment or order if passed by a court of sessions; or

(b) to the court of sessions concerned against such judgment or order if passed by a magistrate.

CHAPTER VI PREVENTIVE MEASURES

48. Prevention of electronic crimes.— (1) The Federal Government or the Authority, as the case may be, may issue directives to be followed by the owners of the designated information systems or service providers in the interest of preventing any offence under this Act.

(2) Any owner of the information system who is not a licensee of the Authority and violates the directives issued under sub-section (1) shall be guilty of an offence punishable, if committed for the first time, with fine which may extend to ten million rupees and upon any subsequent conviction shall be punishable with imprisonment which may extend to six months or with fine or with both:

Provided that where the violation is committed by a licensee of the Authority, the same shall be deemed to be a violation of the terms and conditions of the licensee and shall be treated as such under the Pakistan Telecommunication (Re-organization) Act, 1996.

49. Computer emergency response teams.—(1) The Federal Government may constitute one or more computer emergency response teams to respond to any threat against or attack on any critical infrastructure information systems or critical infrastructure data, or widespread attack on information systems in Pakistan.

(2) A computer emergency response team constituted under sub-section (1) may comprise of technical experts of known expertise officers of any intelligence or agency or any sub-set thereof.

(3) A computer emergency response team shall respond to a threat or attack without causing any undue hindrance or inconvenience to the use and access of the information system or data as may be prescribed.

CHAPTER VII MISCELLANEOUS

50. Relation of the Act with other laws.—(1) The provisions of this Act shall have effect not in derogation of the Pakistan Penal Code, 1860 (Act XLV of 1860), the Code of Criminal Procedure, 1898 (Act V of 1898), the Qanoon-e-Shahadat, 1984 (P.O. No. X of 1984), the Protection of Pakistan Act, 2014 (X of 2014) and the Investigation for Fair Trial Act, 2013 (I of 2013).

(2) Subject to sub-section (1), the provisions of this Act shall have effect notwithstanding anything to the contrary contained in any other law on the subject for the time being in force.

51. Power to make rules.— (1) The Federal Government may, by notification in the official Gazette, make rules for carrying out purposes of this Act.

(2) Without prejudice to the generality of the foregoing powers, such rules may specify, ---

- (a) qualifications and trainings of the officers and staff of the investigation agency and prosecutors;
- (b) powers, functions and responsibilities of the investigation agency, its officers and prosecutors;
- (c) standard , operating procedures of the investigation agency;
- (d) mode and manner in which record of investigation under this Act may be maintained;
- (e) manner to deal with the seized data, information system, device or other articles;
- (f) working of joint investigation teams;
- (g) requirements for seeking permission of the Authority to change, alter or re-programme unique device identifier of any communication equipment by any person for research or any other legitimate purpose;
- (h) procedure for seeking appropriate orders of the Authority for removal, destruction or blocking access to information under this Act;
- (i) constitution of computer emergency response team and the standard operating procedure to be adopted by such team;
- (j) appointment of designated agency having capability to collect real time information;
- (k) manner of coordination between the investigation agency and other law enforcement and intelligence agencies including designated agency;
- (l) for management and oversight of the forensic laboratory;
- (m) qualifications and trainings of the officers, experts and staff of the forensic laboratory;
- (n) powers, functions and responsibilities of the forensic laboratory, its officers, experts and staff;
- (o) standard operating procedures of the forensic laboratory to interact with the investigation agency;
- (p) manner of soliciting and extending international cooperation; and
- (q) matters connected or ancillary thereto.

52. Removal of difficulties.—If any difficulty arises in giving effect to the provisions of this Act, the Federal Government may, within two years of the commencement of this Act and by order

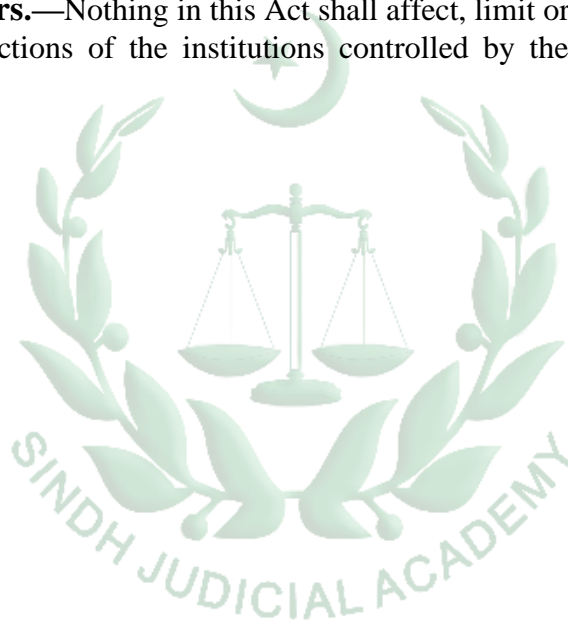
published in the official Gazette, make such provisions not inconsistent with the provisions of this Act as may appear to be necessary for removing the difficulty.

53. Report to Parliament.—The agency designated or established under section 29 of the Act shall submit a half yearly report to both houses of the Parliament for consideration by the relevant Committee in camera, in respect of its activities, without disclosing identity information, in a manner as prescribed under this Act.

54. Amendment of Electronic Transactions Ordinance, 2002 (LI of 2002) and pending proceedings.— (1) Sections 36 and 37 of the Electronic Transactions Ordinance, 2002 (LI of 2002) are omitted.

(2) Any action taken by or with the approval of the Authority or proceedings pending under the provisions of the Electronic Transactions Ordinance, 2002 (LI of 2002) repealed by sub-section (1), shall continue and be deemed to have been taken or initiated under this Act.

55. Savings of powers.—Nothing in this Act shall affect, limit or prejudice the duly authorized and lawful powers and functions of the institutions controlled by the Governments exercised and performed in good faith.



PREVENTION OF ELECTRONIC CRIMES INVESTIGATION RULES, 2018

[Gazette of Pakistan Extraordinary, Part II,

7th August, 2018]

S.R.O. 979(I)/2018, dated 20.7.2018.---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;

(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 the interest of further investigation.

(2) Any unauthorized disclosure of the contents relating to the modesty and dignity of natural persons or tampering 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 years or 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-I8

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 Engineering with (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 years or above computing education) with three years or above experience or BCS (CS) (four years) with five years or 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 counseling 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 logbooks.
- (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 e-mails, 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(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 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.

(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.
- (vii) 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**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	70	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
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

Cybercrimes Reporting Center

Sr. No	Positions	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
8	Assistant Director Laws	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 (P.P.C.) 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.
- (ix) 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 and Time of Receiving	
	Name of the Organizing from which the equipment is received	Name		
		Address		
		Contact No.		
	Type of evidence in the 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;
- (vi) 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	Identity theft	Sexual Exploitation and Abuse	Total

															offence						
	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	
PECA Sections																					
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	Accuses Arrested	Cases Challan ed	Under Trial	Cases Decided	
								Acquitt als	Convict ed
January									
February									
March									
April									
May									
June									
July									
August									

September									
October									
November									
December									
Total									

Reported Case Laws on PECA, 2016

Citation Name : 2023 SCMR 679 SUPREME-COURT

Side Appellant : SHAHZAD

Side Opponent : State

S. 497---prevention of electronic crimes act (XL of 2016), Ss. 21 & 24---Penal Code (XLV of 1860), Ss. 109 & 509---Constitution of Pakistan, Art. 185(3)---Transmitting objectionable photographs and videos through mobile phone---Bail, grant of ---Rule of consistency---Although the petitioner was nominated in the FIR with the specific allegation of transmitting objectionable photographs and videos of the complainant but the record revealed that the sim used for the purpose of transmitting the said photographs and videos was owned by person "A", co-accused, and according to "A" he forgot his sim at the house of person "T", another co-accused---Both "A" and "T" were brother-in-law of the complainant---Although according to the investigation, the mobile phone in which the said objectionable photographs and videos were available, was recovered from the possession of the accused but according to the prosecution while transmitting the said objectionable photographs and videos the sim owned by "A" was used---Bail had already been granted to "A" and in such eventuality, the accused had become entitled to the concession of bail on the principle of rule of consistency---Even otherwise, the accused had no previous criminal record---Petition for leave to appeal was converted into appeal and allowed, and accused was granted bail.

Citation Name : 2023 SCMR 401 SUPREME-COURT
Side Appellant : JAVED IQBAL
Side Opponent : State
<p>Ss. 497 & 499---prevention of electronic crimes act (XL of 2016), Ss. 13 & 14---Penal Code (XLV of 1860), Ss. 420, 468, 471 & 109---Constitution of Pakistan, Art. 185(3)---electronic forgery and fraud---Bail, grant of ---Condition of depositing money in Trial Court for grant of bail---Legality---High Court granted post-arrest bail to accused, subject to his furnishing of bail bonds in the sum of Rs.500,000/- with one surety in the like amount to the satisfaction of the trial Court, and further directed the accused to deposit Rs.3.5 million in the Trial Court---Held, that the High Court without any legal backing imposed the condition of depositing of Rs.3.5 million besides the surety bonds---Petition for leave to appeal was converted into appeal and allowed, the condition imposed by the High Court of depositing of Rs.3.5 million in the trial Court was set-aside and the order of granting post-arrest bail to the accused, subject to his furnishing bail bonds of Rs.500,000/- (Rupees five hundred thousand) with one surety was maintained.</p>
Citation Name : 2023 YLR 1377 PESHAWAR-HIGH-COURT
Side Appellant : NAVEED
Side Opponent : State
<p>Ss. 21 & 24---Criminal Procedure Code (V of 1898), S. 561-A---Modesty of a natural person and cyber stalking---Appreciation of evidence---Explicit content, sending of ---Proof ---Accused was alleged to have transmitted objectionable photograph of complainant to her father with intention to force the family to enter into compromise in another criminal case---Trial Court and Lower Appellate Court convicted and sentenced the accused of the offences---Validity---Motive behind occurrence was reasonably implausibly explained by complainant and her father in their respective statements recorded during trial---Accused had sent explicit content of complainant and messages to her father---Various crimes were addressed by prevention of electronic crimes act, 2016, by the name of Cyber crimes---Such crimes though taking various forms could be broadly classified under the scheme of prevention of electronic crimes act, 2016, as either directly targeting an electronic device or using it to facilitate other crimes---Transmission through an electronic device as well as cyber stalking used to intimidate and influence outcome of a murder charge---Transmission of images was the means to achieve the end goal and charges were laid under Ss. 21 & 24 of prevention of electronic crimes act, 2016, which had been duly proved by prosecution and accused was rightly convicted and sentenced by two forums below---High Court declined to alter factual findings by lower fora at the altar of every doubtful may, as the same carried significant weight---Petition was dismissed, in circumstances.</p>

Citation Name : 2023 PCrLJ 496 PESHAWAR-HIGH-COURT
Side Appellant : FAKHAR ZAMAN
Side Opponent : State
<p>S. 497---prevention of electronic crimes act (XL of 2016), Ss.20, 21 & 24---Dignity of natural person, modesty of natural person and cyber stalking---Bail, refusal of ---Harassing and blackmailing a woman---Complainant alleged that accused had been displaying and transmitting information from his Whatsapp account to harm her reputation and privacy---Validity---Accused not only displayed images and videos but in order to gain financial benefits from complainant, whose husband was abroad had received handsome ransom---Role of accused fell within the preview of definition covered under his implication---In of fences punishable with less than 10 years of imprisonment bails were granted but in appropriate cases it was never compulsion to the Court to grant bail as a rule and could depart from such rule to deny any favour to accused where complainant was helpless, and had been victimized due to her nude images and videos and blackmailed her financially to get illegitimate demand---Complainant was put under extortion of sending her images and nude videos to her husband---Accused sexually harassed complainant who was a married woman while her husband was abroad doing labour for earning livelihood for family---Bail was declined in circumstances.</p>
Citation Name : 2023 PCrLJ 1092 ISLAMABAD
Side Appellant : JAVAD KHAN
Side Opponent : State
<p>Ss. 13, 14, 29 & 30---Penal Code (XLV of 1860), Ss. 419 & 420---Constitution of Pakistan, Art. 199---Constitutional petition---Cyber-crime and cheating---Non-cognizable offences, investigation of ---Two sets of offences---Petitioner sought quashing of FIR with the plea that of fence under S. 14 of prevention of electronic crimes act , 2016, was not a cognizable offence and could not be registered without seeking prior permission form a Court and those under P.P.C. could not be investigated by FIA---Validity---Charge against petitioner was that he was liable for an offence under S. 14 of prevention of electronic crimes act , 2016---In view of S. 43 of prevention of electronic crimes act , 2016, the offence was non-cognizable and consequently FIA could not have taken cognizance of it without seeking prior permission from a Court of competent jurisdiction---This was not done by authorities and cognizance of offence under S. 14 of prevention of electronic crime act , 2016 and steps taken subsequent to such cognizance by FIA were devoid of legal authority---Federal Investigating Agency, as investigation agency designated under S. 29 of prevention of electronic crimes act , 2016, was devoid of authority to investigate of fences under P.P.C. through joinder of such offences with offences under prevention of electronic crimes act , 2016---Federal Investigating Agency could not have therefore registered a complaint under Ss. 419 & 420, P.P.C. and investigate the same---High Court declared that FIA was devoid of legal authority to registered FIR, which was liable to be quashed---Federal Investigating Agency could seek appropriate permission from Court of competent jurisdiction to take cognizance of alleged offence committed by petitioner under S. 14 of prevention of electronic crimes act , 2016---act ions attributed to petitioner constituted of fences under P.P.C. also, therefore, complainant was within his right to file a complaint</p>

with police authorities so that FIR could be registered in exercise of authority under Cr.P.C.--- Constitutional petition was allowed accordingly.

Citation Name : 2023 PCrLJ 1092 ISLAMABAD

Side Appellant : JAVAD KHAN

Side Opponent : State

Ss. 29 & 44---Penal Code (XLV of 1860), Ss. 419 & 420---Two sets of offences, cognizance of --- Principle---Federal Investigating Agency is the designated agency under S. 29 of prevention of electronic crimes act , 2016 and is not vested with jurisdiction to investigate allegations that attract offences under P.P.C., merely because they relate to the actions that attract an offence under prevention of electronic crimes act , 2016---In such case, proviso of S. 30 of prevention of electronic crimes act , 2016, provides for creation of a JIT to facilitate related investigations and at the culmination of such investigation it is for FIA to file a challan before Special Court designated under S. 44 of prevention of electronic crimes act , 2016 and for the police authorities to undertake criminal proceedings and file a challan before a Trial Court competent to take cognizance of an offence under P.P.C.

Citation Name : 2022 SCMR 1511 SUPREME-COURT

Side Appellant : ROHAN AHMAD

Side Opponent : State

S. 497---Penal Code (XLV of 1860), Ss. 295-B, 298-C, 120-B, 34 & 109--- prevention of electronic crimes act (XL of 2016), S. 11---Constitution of Pakistan, Art. 185(3)--- Disseminating religious beliefs of Qadiani faith through social media and the internet---Bail, refusal of ---During investigation it was found that accused used to publicly upload proscribed defiled translation of the Holy Quran, blasphemous books and other material and also created a link to an online storage drive and disseminated it through a WhatsApp number, which was registered against his name---Co-accused used to provide blasphemous content for online competitions through an email address and the number mentioned in that email was registered against his name; he also created a WhatsApp group and used to supervise and pass instructions regarding the quiz competitions through WhatsApp; and he disseminated defiled translation of the Holy Quran through WhatsApp-- -As regards role of the other co-accused, during investigation it was found that he prepared the quiz questions and papers of proscribed material and disseminated the same to the accused and co-accused through his email---Prosecution had sufficient material on record to connect the accused and both the co-accused with the alleged crime and in the circumstances, they were not entitled for grant of bail-- -Petitions for leave to appeal were dismissed, leave was refused, and accused and both co-accused persons were refused bail.

Citation Name : 2022 SCMR 1477 SUPREME-COURT
Side Appellant : ZAHEER AHMAD
Side Opponent : State
<p>S. 497--- Penal Code (XLV of 1860), Ss. 295-A, 295-B, 295-C, 298-C, 34 & 109--- prevention of electronic crimes act (XL of 2016), S. 11---Constitution of Pakistan, Art. 185(3)--- Propagation of Qadiani faith through social media by forwarding material and translation of Holy Quran proscribed by the government---Bail, refusal of ---Accused was nominated in the FIR and he was one of the administrators of the WhatsApp group along with co-accused and forty other persons were also members of the said group---Certain proscribed book and banned text and translation of Holy Quran was shared in the said group---Co-accused disseminated banned material to accused and another co-accused for further sharing with public at large; he also used to provide derogatory books and guidelines to the accused through a WhatsApp number, registered in his name---According to the investigating officers, detailed forensic analysis of cell phones of the accused, and both co-accused was conducted by the Federal Investigation Agency (FIA) and it was found that, the accused, being one of the administrator of the WhatsApp group, used to add and remove persons not belonging to Ahmadi community in the group on the instructions of co-accused---Sufficient incriminating material was available on record connecting the accused and co-accused with the commission of alleged offence---Petitions for leave to appeal were dismissed, leave was refused and accused and co-accused were refused bail.</p>

Citation Name : 2022 PLD 773 LAHORE-HIGH-COURT-LAHORE
Side Appellant : MEERA SHAFI
Side Opponent : FEDERATION OF PAKISTAN
<p>Art. 19---prevention of electronic crimes act (XL of 2016), S. 20---Freedom of speech---offences against dignity of a natural person---Scope---Petitioners attacked the constitutionality of S. 20 of prevention of electronic crimes act , 2016, (PECA) on the ground that defamation is not among the restrictions imposed by the legislature in Art. 19 of the Constitution and does not have even a proximate connection with any of them---Petitioner also pointed out that the original Art. 19 (as it stood in the 1973 Constitution) included defamation in the list but it was omitted later on---Validity---Fundamental rights essentially afford protection against contraventions by the State and its instrumentalities---Wrong of defamation is not a public but a private wrong---Legislature is competent to make a law relating to defamation even under the amended Art. 19---Section 20 of prevention of electronic crimes act , 2016, may also be justified on the ground that defamation and libel may endanger public order and incite an offence-the interests expressly protected under Art. 19 of the Constitution---Parliament was competent to enact S. 20 of prevention of electronic crimes act , 2016.</p>

Citation Name : 2021 PCrLJ 506 PESHAWAR-HIGH-COURT

Side Appellant : Professor AKHTAR KHAN

Side Opponent : State

S. 497---prevention of electronic crimes act (XL of 2016), Ss. 10 & 11---Penal Code (XLV of 1860), S. 109---Cyber terrorism, hate speech and abetment--- Bail, grant of ---Delayed FIR---Further inquiry---Scope---Accused was alleged to have been found involved in sharing hate speech and fake information against Government institutions through his Facebook/Twitter accounts---Sections 10 & 11 of prevention of electronic crimes act , 2016, were punishable with imprisonment or fine or both---If at trial, the accused was only sentenced with fine then his period as under trial prisoner due to refusal of bail would amount to double jeopardy---Lesser sentence had to be taken into consideration for the purpose of grant of bail---Complaint was made after four months of the occurrence---Identity created on Social Media was purportedly of the accused but actual usage by the accused was a question of evidence which could only be determined at trial---Case of accused was one of further inquiry---Accused was not required for the purpose of investigation---Petition for grant of bail was allowed.

Citation Name : 2021 PCrLJ 1457 KARACHI-HIGH-COURT-SINDH

Side Appellant : ADIL NADEEM

Side Opponent : State

S. 497---prevention of electronic crimes act (XL of 2016), S. 22---Child pornography---Bail, refusal of ---Delayed FIR---Scope---Prosecution case was that a cyber crime operation was launched abroad to fight the diffusion of child sexual abuse material through social media groups in which 351 foreign numbers were investigated; one of them being that of accused, FIA raided the house of accused, seized his cell phone as well as two computer hard drives---Seized drives were sent for forensic analysis and images/videos of minors were found---Accused contended that the FIR was lodged after 3 years; that the images/videos were uploaded by his brother who had died and that the offence with which he was charged did not fall within the prohibitory clause of S. 497, Cr.P.C.--Telephone number identified by the Interpol was admittedly in use of the accused nor the recoveries were denied---Fact that gangs from all over the world were investigated, their respective details were obtained and then traced back to the individual countries from where the child pornography originated justified the delay---Fact that the accused was in exclusive use of equipment for the last few years and had taken pains to install application locking passwords on the same, required deeper analysis of evidence---High Court observed that behaviour would be repeated if bail was granted or that the accused would abscond---Nature of accusations and the material collected to date merited the case to fall within the exception of granting bail when the offence fell within the non-prohibitory clause of S. 497, Cr.P.C.--- Application for grant of bail was dismissed, in circumstances.

Citation Name : 2021 PCrLJ 119 KARACHI-HIGH-COURT-SINDH

Side Appellant : SALEEM KHALID

Side Opponent : State

S. 497---prevention of electronic crimes act (XL of 2016), Ss. 20, 21 & 24---offences against dignity of natural person, offences against modesty of a natural person and minor, cyber stalking---Bail, refusal of ---Recovery of incriminating material on pointation of accused---Scope---Accused was alleged to have shared obscene videos of his ex-wife within and outside her family---FIA officials had proceeded to the house of accused and got recovered on pointation, the incriminating paraphernalia which was seized in presence of witnesses under a seizure memo.---Accused person's admission of making videos gave weight to the allegations that by making videos and photographs he forced the complainant to indulge into obscene activities with his friends which he recorded and that the accused later on used her explicit images and videos to control, blackmail and force her to perform other sexual activities---Sections 20, 21 & 24 of prevention of electronic crimes act, 2016 did not fall within the prohibitory clause of S. 497, Cr.P.C. but in such like cases where dignity and modesty of a person was at stake, the discretion for grant of bail had to be exercised cautiously---Prosecution had sufficient material against the accused to connect him with the commission of alleged offence---Petition for grant of bail was dismissed.



Case Laws on Prevention of Electronic Crimes Investigation Rules, 2018

Citation Name : 2022 PLD 773 LAHORE-HIGH-COURT-LAHORE

Side Appellant : MEERA SHAFI

Side Opponent : FEDERATION OF PAKISTAN

Ss. 155 & 537---Prevention of Electronic Crimes Investigation Rules, 2018, R. 7---Information in non-cognizable cases---Investigation and case procedure---Scope---Petitioners claimed that R. 7(5) of the Prevention of Electronic Crimes Investigation Rules, 2018, has not been followed---Validity---Even if it is assumed that the petitioners' stance is correct, they cannot get any benefit because there is nothing on the record which may suggest that they have been prejudiced or the officers of investigating authority were dishonest or had malice against them---Any irregularity or defect in investigation stands cured under S. 537, Cr.P.C.

Citation Name : 2022 PLD 773 LAHORE-HIGH-COURT-LAHORE

Side Appellant : MEERA SHAFI

Side Opponent : FEDERATION OF PAKISTAN

Ss. 155 & 154---Prevention of Electronic Crimes Investigation Rules, 2018, Rr. 6 & 7---Information in non-cognizable cases---Investigation and case procedure---Scope---Rule 6(3) of Prevention of Electronic Crimes Investigation Rules, 2018, (PECIR) stipulates that a complainant may file his complaint in-person, via e-mail, fax, telephone or other available digital means to a Cybercrime Reporting Centre---Rule 7 retains the distinction between cognizable and non-cognizable offences--
-However, it is not happily worded and appears to be incoherent---Rule 7(1) lays down that the Circle in-charge may allow registration of a case on the complaint received under R. 6(3) and nominate an investigation officer while R. 7(4) enjoins that if the offence alleged in the complaint is cognizable, the Circle in-charge shall order registration of case after seeking legal opinion and approval of the Additional Director in the zone---On the other hand, R. 7(5) ordains that non-cognizable offences are to be dealt with according to S. 155, Cr.P.C. and permission of the competent court is necessary for their investigation---Tension between different provisions of R. 7 can be resolved by holding that when a complaint is received at the Cybercrime Reporting Centre the Circle in-charge may allow it to be registered for further processing and nominate an officer therefor---First Information Report is to be lodged only if it is found that a cognizable offence has been committed under the PECA and that too after completing the requirements of R. 7(4) but in the case involving non-cognizable offence the Circle in-charge should seek permission of the competent court for investigation.





THE FEDERAL INVESTIGATION AGENCY ACT, 1974



CONTENTS

SECTIONS:

1. Short title, extent and commencement
2. Definitions
3. Constitution of the Agency
4. Superintendence and administration of the
5. Powers of the members of the Agency
- 5-A. Certain Officers of the Agency deemed to be Public Prosecutors
6. Power to amend the Schedule
7. Delegation of powers
8. Indemnity
9. Power to make rules
10. Repeal

FEDERAL INVESTIGATION AGENCY ACT, 1974

¹ACT No. VIII OF 1975

[13th January, 1975]

An Act to provide for the constitution of a Federal Investigation Agency

WHEREAS it is expedient to provide for the constitution of a Federal Investigation Agency for the investigation of certain offences committed in connection with matters concerning the Federal Government, and for matters connected therewith;

It is hereby enacted as follows: —

1. Short title, extent and commencement.—(1) This Act may be called the Federal Investigation Agency Act, 1974.

(2) It extends to the whole of Pakistan and also applies to all citizens of Pakistan and public servants, wherever they may be.

(3) It shall come into force at once.

2. Definitions. In this Act, unless there is anything repugnant in the subject or context,—

- (a) “Agency” means the Federal Investigation Agency constituted under section 3;
- (b) “Code” means the Code of Criminal Procedure, 1898 (Act V of 1898);
- (c) “Director-General” means the Director-General of the Agency;
- (d) “Provincial Police” means the Police constituted by a Provincial Government under the Police Act, 1861 (V of 1861);
- (e) “public servant” means a public servant as defined in section 21 of the Pakistan Penal Code (Act XLV of 1860), and includes an employee of any corporation or other body or organization set up, controlled or administered by ¹⁵ ¹⁶[, or under the authority of,] the Federal Government;
- (f) “Special Police” means the Pakistan Special Police Establishment constituted under the Pakistan Special Police Establishment Ordinance, 1948 (VIII of 1948);
- (g) “specified persons” means the persons who were appointed to posts in or under a Provincial Police in pursuance of Article 3 of the Special Police and Provincial Police (Amalgamation) Order, 1962 (P. O. No. 1 of 1962); and
- (h) “rules” means rules made under this Act.

¹For Statement of Objects and Reasons, see Gaz. of P., 1974, Ext., Pt. III, p.1385.

¹⁵Applied to PATA (NWFP), see NWFP Gaz. Ext., dated 26-5-2000.

¹⁶Ins. by the Prevention of Corruption Laws (Amdt.) Act, 1977 (13 of 1977), s.2 and Sch.,

3. Constitution of the Agency. — (1) Notwithstanding anything contained in any other law for the time being in force, the Federal Government may constitute an Agency to be called the Federal Investigation Agency for inquiry into, and investigation of, the offences specified in the Schedule, including an attempt or conspiracy to commit, and abetment of, any such offence.

(2) The Agency shall consist of a Director General to be appointed by the Federal Government and such number of other officers as the Federal Government may, from time to time, appoint to be members of the Agency.

4. Superintendence and administration of the Agency.—(1) The superintendence of the Agency shall vest in the Federal Government.

(2) The administration of the Agency shall vest in the Director-General who shall exercise in respect of the Agency such of the powers of an Inspector-General of Police under the Police Act, 1861 (V of 1861), as may be prescribed by rules.

5. Powers of the members of the Agency.—(1) Subject to any order which the Federal Government may make in this behalf, the members of the Agency shall, for the purpose of an inquiry or investigation under this Act, have throughout Pakistan such powers, including powers relating to search, arrest of persons and seizure of property, and such duties, privileges and liabilities as the officers of a Provincial Police have in relation to the investigation of offences under the Code or any other law for the time being in force.

(2) Subject to rules, if any, a member of the Agency not below the rank of a Sub-Inspector may, for the purposes of any inquiry or investigation under this Act, exercise any of the powers of an officer-in-charge of a police-station in any area in which he is for the time being 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 station.

(3) Without prejudice to the generality of the provisions of sub-section (1) and sub-section (2), any member of the Agency not below the rank of a Sub-Inspector authorized by the Director-General in this behalf may arrest without warrant any person who has committed, or against whom a reasonable suspicion exists that he has committed, any of the offences referred to in sub-section (1) of section 3.

(4) For the purpose of the exercise by the members of the Agency of the powers of an officer in charge of a police-station, “Police-station” includes any place declared, generally or specially, by the Federal Government to be a police-station within the meaning of the Code.

(5) If, in the opinion of a member of the Agency conducting an investigation, any property which is the subject-matter of the investigation is likely to be removed, transferred or otherwise disposed of before an order of the appropriate authority for its seizure is obtained, such member may, by order in writing, direct the owner or any person who is, for the time being, in possession thereof not to remove, transfer or otherwise dispose of such property in any manner except with the previous permission of that member and such order shall be subject to any order made by the Court having jurisdiction in the matter.

(6) Any contravention of an order made under sub-section (5) shall be punishable with rigorous imprisonment for a term which may extend to one year, or with fine, or with both.

[5-A. Certain Officers of the Agency deemed to be Public Prosecutors. Notwithstanding anything contained in any other law for the time being in force the Assistant Directors (Legal) and the Deputy Directors (Law) of the Agency shall be deemed to be Public Prosecutors and shall be competent to institute and conduct any proceedings in cases sent up for trial by the Agency in the Special Courts

constituted under any law and the courts subordinate to the High Court.]

6. Power to amend the Schedule. The Federal Government may, by notification in the official Gazette, amend the Schedule so as to add any entry thereto or modify or omit any entry therein.

7. Delegation of powers. The Director-General may, by order in writing, direct that all or any of his powers under this Act or the rules shall, subject to such conditions, if any, as may be specified in the order, be exercisable also by any member of the Agency so specified.

8. Indemnity. No suit, prosecution or other legal proceeding shall lie against the Federal Government, any member of the Agency or any other person exercising any power or performing any function under this Act or the rules for anything which is in good faith done or intended to be done under this Act or the rules.

9. Power to make rules. — (1) The Federal Government may, by notification in the official Gazette, make rules¹ for carrying out the purposes of this Act.

(2) In particular and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:—

- (a) the terms and conditions of service of the Director-General and other members of the Agency and the qualifications for recruitment to various posts;
- (b) the powers and functions of the members of the Agency in relation to the conduct of inquiries and investigations;
- (c) the nature and extent of the assistance which the Agency may provide to Provincial investigating agencies;
- (d) the powers of the Inspector-General of Police under the Police Act, 1861 (V of 1861), which shall be exercisable by the Director-General; and
- (e) the manner in which rewards may be given to the members of the Agency or of the public for rendering commendable services.¹⁷

10. Repeal.—(1) The Pakistan Special Police Establishment Ordinance, 1948, (VIII of 1948), and the Special Police and Provincial Police (Amalgamation) Order, 1962 (P. O. No.1 of 1962), hereinafter referred to respectively as the said Ordinance and the said Order, are hereby repealed.

(2) Upon the repeal of the said Ordinance,—

- (a) all persons who were members of the Special Police immediately before such repeal, including the specified persons, shall stand transferred to the Agency and shall, subject to sub-section (5), be entitled to the same terms and conditions to which they were entitled immediately before such repeal; and
- (b) any inquiry or investigation pending with the Special Police immediately before

¹⁷Ins. by the Federal Investigation Agency (Amdt.) Ord. (109 of 02), s.2.

such repeal shall continue to be conducted by the Agency.

(3) Notwithstanding the repeal of the said Order, but subject to sub-section (4), every specified person shall continue to be appointed in or under the provincial Police in or under which he was holding a post immediately before the commencement of this Act.

(4) On the recommendation of the Director-General, and with the concurrence of the Provincial Government concerned, the Federal Government may direct that such of the specified persons referred to in sub-section (3) as may, within thirty days of the commencement of this Act, express their willingness to serve in or under the Agency shall be appointed to posts in or under the Agency. ¹⁸

(5) A specified person referred to in clause (a) of sub-section (2), and a person in respect of whom a direction is issued under sub-section (4) shall, upon the repeal of the said Ordinance or, as the case may be, the issue of such direction, cease to hold a post in or under the Provincial Police concerned and shall be entitled to the same terms and conditions of service to which he was entitled immediately before such repeal or the issue of such direction.



THE SCHEDULE

[See sections 3(1) and 6]

(1) Offences punishable under sections ^a[120-B, 121, 122, 123, 123-A, 124, 124-A], ^g[161, 162, 163, 164, 165, 165-A, 168, 169], ^d[175, 182, 183, 186, 187, 188, 189], ^c[201], ^e[216], ^b[217, 218], ^e[223], ^d[224, 225], ^e[225-A], ^e[245], ^b[255, 256, 257, 258, 259, 260, 261, 263], ^f[295-A] ^x[295-B] ^f[295-C, 298, 298-A], ^a[300, 301, 302, 324, 332, 333, 334, 335, 336, 337, 337-A, 337-B, 337-C, 337-D, 337-E, 337-F], ^d[342, 348], ^b[353], ^a[365-A], ^b[366-B], ^d[383], ^b[402-A, 402-B, 402-C, 403, 404], ⁱ[406], ^c[407, 408], ^b[409], ^c[411, 418, 419], ⁱ[420], ^a[435, 436, 440], ^k[462A, 462B, 462C, 462D, 462E, 462F], ^l[462H, 462I, 462J, 462K, 462L, 462M], ^d[466], ^c[467], ⁱ[468, 471], ^c[472], ^d[473, 474, 475, 476], ^b[477-A, 489-A, 489-B, 489-C, 489-D, 489-E], ^j[489-F], ^d[499, 500, 501, 502] ^x[505] ^d[506, 507], of the Pakistan Penal Code (Act XLV of 1860).

^m[1-A] Section 25-D and Section 29 of Telegraphic Act, 1885.

^b[2] Offences punishable under the Explosive Substance Act, 1908 (VI of 1908).

^b[3] Offences punishable under the Official Secret Act, 1923 (XIX of 1923).

^b[4] Offences punishable under the Foreigners Act, 1946 (XXXI of 1946).

^b[5] Offences punishable under the Prevention of Corruption Act, 1947 (II of 1947).

^b[6] Offences punishable under the Foreign Exchange Regulation Act, 1947.

^b[7] Offences punishable under the Import and Export (Control) Act, 1950 (XXXIX of 1950).

^b[8] Offences punishable under Banking Companies Ordinance, 1962 (LVII of 1962).

^b[9] Offences punishable under the Pakistan Arms Ordinance, 1965 (W.P. Ord XX of 1965).

^b[10] Offences punishable under section 156 of the Customs Act, 1969 (IV of 1969).

^b[11] Offences punishable under the Foreign Exchange Repatriation Regulation, 1972.

^b[12] Offences punishable under the Foreign Assets (Declaration) Regulation 1972.

^b[13] Offences punishable under the National Registration Act 1973 (LVI of 1973). (Omitted)

^b[14] Offences punishable under the High Treason (Punishment) Act, 1973 (LXVIII of 1973).

^b[15] Offences punishable under the Prevention of Anti-National Activities Act, 1974 (VII of 1974).

^b[16] Offences punishable under the Banks (Nationalization) Act, 1974 (XIX of 1974).

^b[17] Offences punishable under the Passport Act, 1974 (XX of 1974).

^b[18] Offences punishable under the Drugs Act, 1976 (XXXI of 1976).

^b[19] Offences punishable under Emigration Ordinance, 1979 (XVIII of 1979).

^b[20] Offences punishable under the Exit from Pakistan (Control) Ordinance, 1981 (XLVI of 1981).

^a[21] Offences punishable under the Anti-Terrorism Act, 1997 (XXVII of 1997) to the extent of dealing with cases which:

[1] have Inter-provincial scope, or

[2] are entrusted to the Agency by the Federal Government

^o[22] Offences punishable under the Prevention & Control of Human Trafficking Ordinance 2002.

^p[23] Offences punishable under the Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996).

^q[24] Offences punishable under the National Database and Registration Authority Ordinance, 2002.

^r[25] Offences punishable under Section 36 & 37 of the Electronic Transmission Ordinance, 2002 (LI of 2002).

- ^s[26] Offences punishable under the Copyright Ordinance, 1962 (XXXIV of 1962).
^t[27] Offences punishable under the Prevention of Electronic Crime Ordinance 2007.
^u[28] Offences punishable under the Anti-Money Laundering Ordinance, 2007 (XLV of 2007).
^v[29] Offences punishable under the Electricity Act, 1910 (IX of 1910).
^w[30] Offences punishable under the Protection of Pakistan Act, 2014 (X of 2014).
^x[31] Offences punishable under the Anti-Money Laundering Act, 2010 (VII of 2010).
^y[32] Offences punishable under the Prevention of Electronic Crime Act, 2016.
^z[33] Offences punishable under the Transplantation of Human Organs and Tissues act, 2010.
^z[34] Offences punishable under the Prevention of Smuggling of Migrant Act, 2018 (XXVIII of 2018).
^z[35] Offences punishable under the Prevention of Trafficking in persons Act, 2018 (XXXIV of 2018).
^z¹[36] Offences punishable under Public Properties (Removal of Encroachment) Ordinance, 2021(Ord No. XVI of 2021).

AUTHORITY

- a. S. R. O. 704 (I)/2004. dated 18 August 2004, [693 (2004)/Ex. Gaz.] [F. No. 4/14/2003-POLL (2)]
- b. S. R. O. 826(I)/97 dated 20 September 1997, [No. 1/18/97-FIA.I.]
- c. S. R. O. 113(I)/2002 dated 18 February 2002, [128(2002)/Ex. Gaz.]
- d. S. R. O. 381(I)/2012 dated 18 April 2012, [2428(2012)/Ex. Gaz.] [No. 7/13/2012-FIA.]
- e. S. R. O. 31(KE)/15, dated 22 December 2014, [No. 1/12/2014-FIA]
- f. S. R. O. 620(I)/2018, dated 18 May 2018 , [5925(2018)/Ex. Gaz.] [No. 1/2/2017-FIA]
- g. [Entry 161, 162, 163, 164, 165, 165-A, 168, 169 omitted by SRO 702(1) 2004 dated 16.08.2004
PLD 2004 Cent. St. Sup. 649 Inst. By SRO 1097(I)/2008, dated 24.10.2008, PLD 2004-2009 Supp. Fed. St. 125]
- h. Section 409 omitted by 702(1) 2004 dated 16.08.2004, PLD 2004 Cent St. Sup. 649 Inst. By S.R.O 1097(I)/2008, dated 24.10.2008, PLD 2004-2009 Supp. Fed. St. 125.
- i. S. R. O. 237(I)/98 dated 10 April 1998, [No. 1/18/97-FIA]
- j. S. R. O. 977(I)/2003 dated 9 October 2003, [5187 (2003)/Ex. Gaz.] [F. No. 1/18/97-FIA.I.]
- k. S. R. O. 67(KE)/2013 dated 03 September 2013, [F. No. 1/4/2013-FIA]
- l. S. R. O. 1047(I)/2016 dated 10 November 2016 [4012(2016)/Ex. Gaz.] [1/2/2016- (FIA).]
- m. S. R. O. 1231(I)/2012 dated 1 October 2012, [3038(2012)/Ex. Gaz.] [F. No. 7/13/2012-FIA.]
- n. S. R. O. 157(I)/2002 dated 19 March 2002 , [215(2002)/Ex. Gaz.] S. R. O. 157(I)/2002 dated 19 March 2002, [215(2002)/Ex. Gaz.]
- o. S. R. O. 741(I)/2002 dated 26 October 2002, [1249(2002)/Ex. Gaz.] [F. No. 1/18/97-FIA.I.]
- p. S. R. O. 853(I)/2002 dated 28 November 2002, [1411(2002)/Ex. Gaz.] [F. No. 1/12/2002-FIA.I.]
- q. S. R. O. 549(I)/2003 dated 18 June 2003, [4897(2003)/Ex. Gaz. [F. No. 1/11/2002-FIA.I.]
- r. S. R. O. 1050(I)/2003 dated 15 November 2003, [F. No. 1/18/97-FIA.I.]
- s. S. R. O. 321(I)/2005 dated 19 April 2005, [2800(2005)/Ex. Gaz.] [F. No. 1(I)/2005-FIA.I.]
- t. S. R. O. 206(I)/2008 dated 04 March 2008, [2213(2008)/Ex. Gaz.]
- u. S. R. O. 1097(I)/2008 dated 21 October 2008, [3120(2008)/Ex. Gaz.] [F. No. 1/154/2001/FIA]
- v. S. R. O. 1/4/2013-FIA dated 24 July 2013 [F. No. 1/3/2013-FIA, dated 16 July 2013]

- w. S. R. O. 5(KE)/2016 dated 7 January 2016, [F. No. 1/5/2015-(FIA)]
- x. MOI Notification No. [F. No. 4/24/2022-FIA, dated 3rd November 2022]
- y. S. R. O. 353(I)/2017 dated 20 May 2017 [706(2017)/Ex. Gaz.], [No. 1/2017-FIA]
- z. MOI Notification No. [F. No. 1/4/2018-FIA dated 23 August, 2021] z/1.
MOI Notification No. [F. No. 1/4/2018-FIA dated 29th October, 2021]



Federal Investigation Rules, 1975

S.R.O. 130 (1)/75, dated 29th January, 1975: In exercise of the powers conferred by sub-section (1) of Section 9 of the Federal Investigation Agency Act, 1974, the Federal Government is pleased to make the Following rules:---

1. Short title and commencement: (1) These rules may be called the Federal Investigation Rules, 1975.

(2) They shall come into force at once.

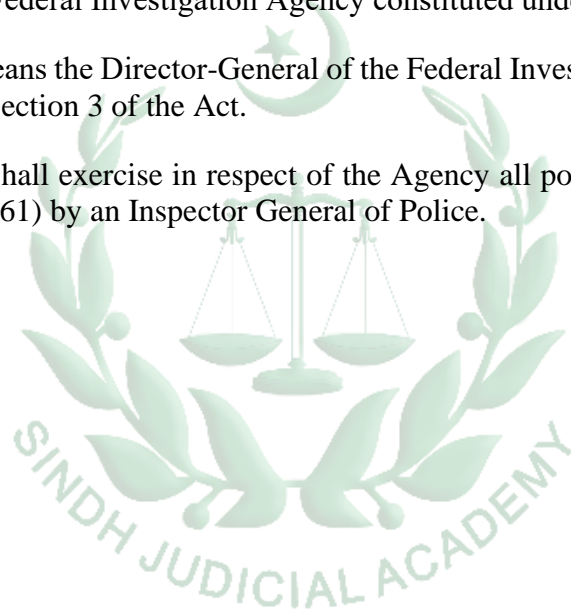
2. Definitions: In these rules, unless there is anything repugnant in the subject or the context:---

(a) “Act” means the Federal Investigation Agency Act, 1974;

(b) “Agency” means the Federal Investigation Agency constituted under the Act; and

(c) “Director-General” means the Director-General of the Federal Investigation Agency appointed under sub-section (2) of Section 3 of the Act.

3. The Director-General shall exercise in respect of the Agency all powers exercisable under the Police Act, 1861 (V of 1861) by an Inspector General of Police.



Federal Investigation Agency (Inquiries and Investigations) Rules, 2002

[Gazette of Pakistan, Extraordinary, Part II, 27th August, 2002]

S.R.O. 567(I)/2002, dated 23-8-2002.--In exercise of the powers conferred by subsection (1) of section 9 of the Federal Investigation Agency Act, 1974 (VIII of 1975), the Federal Government is pleased to make the following rules, namely:---

1. Short title and commencement.--(1) These Rules may be called, the Federal Investigation Agency (Inquiries and Investigations) Rules, 2002.

(2) They shall come into force at once.

2. Definitions.--(1) In these rules unless there is anything repugnant in the subject or context,---

(a) "Act" means the Federal Investigation Agency Act, 1974 (VIII of 1975):---

(b) "Additional Secretary" means the Additional Secretary, Ministry of Interior, Government of Pakistan;

(c) "competent authority" means the authority to accord permission either to hold an inquiry or investigation, or to order registration of a criminal case, or drop the case after, investigation, or decide departmental proceedings under the Rules;

(d) "Council" means the Federal Anti-Corruption Council (FACC);

(e) "Deputy Director" means the Deputy Director of the Agency;

(f) "Director" means the zonal and functional Director of the Agency;

(g) "Head of Department" means an officer incharge of a Department of the Federal Government, corruption or an autonomous body established by the Federal Government;

(h) "prosecution sanctioning authority" means the Federal Government or, as the case may be, a Provincial Government which may sanction for prosecution under section 197 of the Code of Criminal Procedure, 1898 (Act V of 1898), or, as the case may be, under subsection (5) of section 6 of the Pakistan Criminal Law Amendment Act, 1958 (XL of 1958); and

(i) "Secretary" means the Secretary, Ministry of Interior, Government of Pakistan.

(2) The words and expressions used but not herein defined shall have the meanings assigned to them in the Act.

3. Initiation of action by the Agency.--(1) The Agency may, subject to rules 4 and 5, initiate an inquiry or investigation either on its own initiative or on receipt of a complaint or oral or written information.

(2) After an inquiry or investigation has been registered, the inquiry of investigation shall proceed with care and discretion and no undue publicity shall be given to it. Special care shall be taken to ensure that no unnecessary damage is caused to the prestige, reputation and dignity of any public servant involved in the case.

4. Verification of complaints against public servants.--The Deputy Director or an officer above the rank of Deputy Director may initiate verification of a complaint in order to ascertain the identity of the complainant or informer and genuineness of the complaint or information. No action shall be taken on any anonymous or pseudonymous complaint.

5. Initiation of inquiry and registration of criminal case.--(1). An inquiry shall be initiated against an accused public servant specified in column (2) of table below with prior permission of the authority, specified in column (3) of that table.

TABLE

S. No	Basic Pay Scale of public servant	Authority
(1)	(2)	(3)
1.	BPS 1-12 and equivalent	Deputy Director
2.	BPS 13-17 and equivalent	Director
3.	BPS 18-19 and equivalent	Director-General
4.	BPS 20-21 and equivalent	Secretary
5.	BPS 22 and equivalent	FACC

(2) Subject to sub-rule (3), a criminal case shall be registered against an accused public servant specified in column (2) of table below with prior permission of the authority specified in column (3) of that table.

TABLE

S. No.	Basic Pay Scale of public servant	Authority
(1)	(2)	(3)
1.	BPS 1-12 and equivalent	Director
2.	BPS 13-17 and equivalent	Director-General
3.	BPS 18-19 and equivalent	Additional Secretary
4.	BPS 20-21 and equivalent	Secretary
5.	BPS 22 and equivalent	FACC

(3) No prior permission under sub-rule (2) shall be required for registration of case against a public servant caught as a result of trap arranged by the Agency under the supervision of a Magistrate of the First Class. In such case, report within twenty four hours shall be made to the Secretary of the Ministry or Division concerned or the Head of the Department concerned and immediate superior of the public servant concerned.

(4) If on receipt of a complaint, the competent authority decides not to initiate an inquiry or register a case, it shall record reasons therefore.

6. Report regarding registration of case and arrest.--The Registration of a case and consequential arrest of a public servant shall be reported to the Head of the Department of the accused within twenty-four hours.

7. Power to call for record of case.---(1) The Secretary and Director General may suo motu or otherwise call for the record of any case or inquiry, pending with the Agency, for examination and give such directions as may be necessary for the speedy, fair and just disposal of the case.

(2) A Director may suo motu or otherwise call for the record of any case or inquiry for the purpose of satisfying himself as to the correctness or propriety of decision taken by a Deputy Director under these rules and may pass such orders as he may be deem lit.

8. Power to drop case and recommend departmental proceeding.---(1) The authority specified in column (3) of the table below may drop a case and recommend departmental proceedings in respect of a public servant specified in column (2) of that table.

TABLE

S. No	Basic Pay Scale of public servant	Authority
(1)	(2)	(3)
1	BPS 1-16 and equivalent	Director-General
2	BPS 17 and equivalent	Additional Secretary
3	BPS 18-19 and equivalent	Secretary
4	BPS 20-22 and equivalent	FACC

(2) When decision to hold departmental proceedings against a public servant is taken under sub-rule (1), the Agency shall forward facts of the case, statement of allegations, list of witnesses and documents if any to the concerned competent authority of the accused public servant for initiating departmental proceedings.

9. Federal Anti-Corruption Council.---(1) There shall be a Federal Anti-Corruption Council (FACC) which shall consist of;

- | | | |
|-----|---|----------|
| (a) | Secretary | Chairman |
| (b) | Representative of the Law, Justice and Human Rights Division not below the rank of Joint Secretary. | Member |
| (c) | Representative of the Establishment Division not below the rank of Joint Secretary. | Member |
| (d) | Director-General, FIA | Member |

(2) The Director-General, Federal Investigation Agency, shall act as Secretary of the Council.

(3) The Federal Anti-Corruption Council shall co-opt a representative of the concerned Ministry (not below the rank of Joint Secretary) whose officer's case is before the Council.

10. Obtaining Sanction for prosecution.---(1) On completion of an investigation, a case found fit for prosecution for which sanction for prosecution is required under section 197 of the Code of

Criminal Procedure, 1898 (Act V of 1898), or under subsection (5) of section 6 of the Pakistan Criminal Law Amendment Act, 1958 (XL of 1958), or the rules made thereunder, shall be submitted by the Agency to the Federal Government to accord sanction of prosecution alongwith full facts of the case, the opinion of the Legal Officer and statement of allegations.

(2) In cases registered against officers working in BPS-20 and above, explanation of the accused officer, giving him fifteen days time shall be obtained by the Director-General. Questions asked and replies furnished by the concerned officer shall invariably be incorporated in the Confidential Final Report and shall be submitted to the Federal Anti-Corruption Council alongwith relevant documents.

(3) In cases of officers working in BPS-19 and below, the prosecution sanctioning authority shall communicate full facts of the case and statement of allegations to the Ministry or Department under whom the public servant concerned is employed. The Ministry or Department shall supply these documents to the public servant concerned and give him an opportunity to submit his reply within thirty days of its receipt.

(4) The Ministry or Department concerned to whom a case has been sent under sub-rule (3) shall convey its recommendations alongwith the statement of the public servant concerned to the prosecution sanctioning authority within sixty days of its receipt.

(5) The prosecution sanctioning authority shall take into consideration the explanation of the accused public servant while making a decision regarding disposal of the case.

(6) If the prosecution sanctioning authority decides to prosecute the accused public servant, sanction for prosecution under section 197 of the Code of Criminal Procedure, 1898 (Act V of 1898), or, as the case may be subsection (5) of section 6 of the Pakistan Criminal Law Amendment Act, 1958 (XL of 1958), shall be given forthwith.

(7) If it is decided to hold departmental proceedings against the public servant, it shall be held by the authority under whom the public servant is serving. The Ministry of Interior, Government of Pakistan or, as the case may be the Agency, shall supply all material required for the departmental proceedings to the concerned Ministry, Division or Department under which the public servant concerned is employed.

11. Competent authority in cases where senior public servant is involved alongwith junior public servant.---If more than one public servant is involved in a case, the competent authority for the public servant in the highest rank shall also be the competent authority for the junior public servant involved in the case.

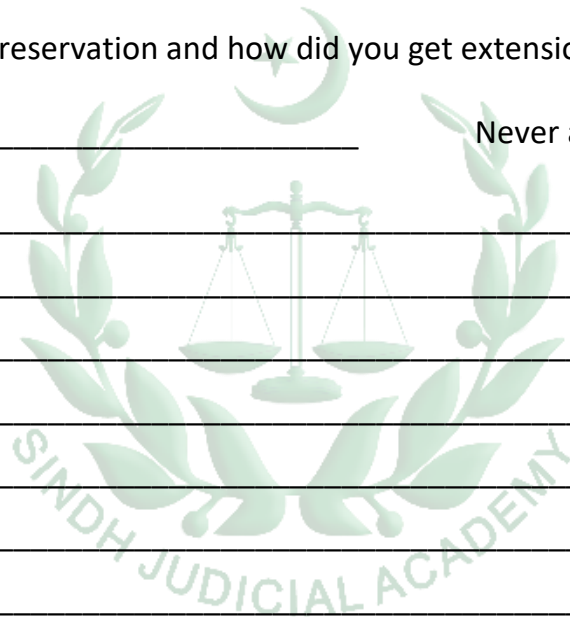
Under the Prevention of Electronic Crimes Act, 2016 term 'Authority' has been defined. What are their powers and responsibility? Identify relevant Section/s and Rule/s.

What was the request format used by you?

Never used

What was the time of preservation and how did you get extension?

Never applied for



Can an investigation agency ask to service provider to provide last 10 months data?

Yes

No

Identify relevant law and explain its procedure.



Sindh Judicial Academy

What would be your response if it is not provided on the ground of non-availability?

Do not know

How many times you requested court for issuance of warrant and seizure of data and devices?

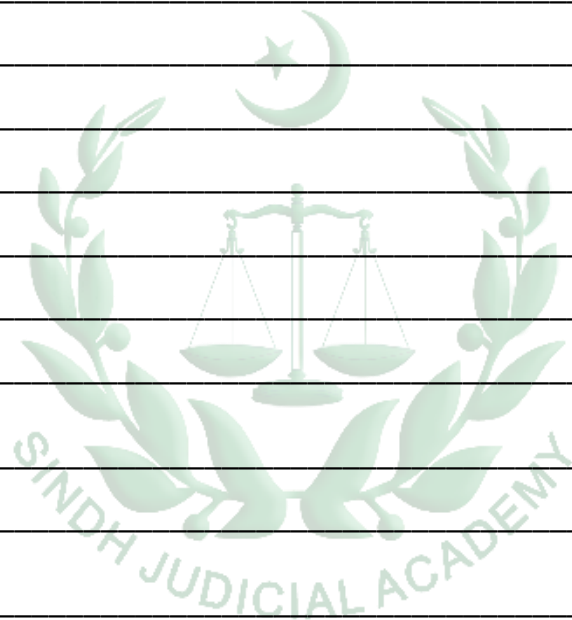
What was its procedure? Draft request letter.

circumstances for search or seizure; who submitted for approval?

Never prepared

Never prepared and filed

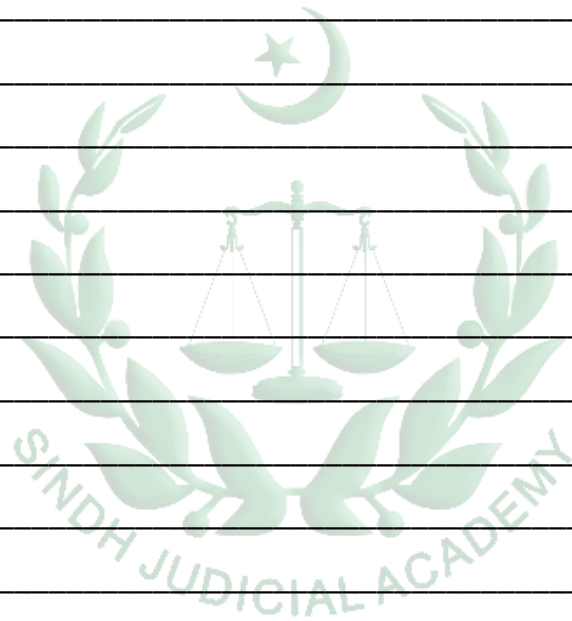
Never prepared and filed



Can an investigation officer compel a person to disclose contents of data? If so, what would be its procedure?

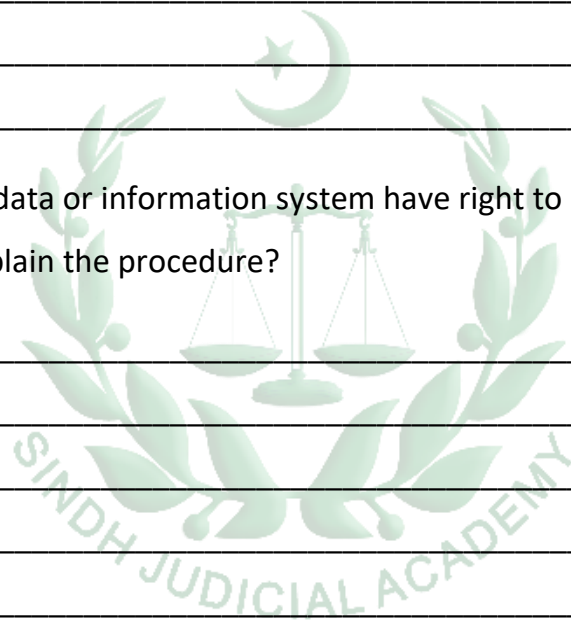


What are the powers of authorized officer under the Prevention of Electronic Crimes Act, 2016?



How data or information system is seized and what is relevant Law?

Does the owner of the data or information system have right to apply for forensic report/images if so, explain the procedure?





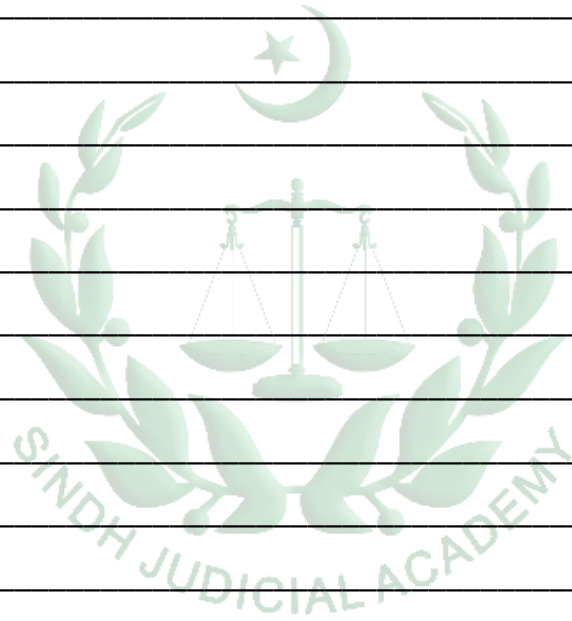
Page 10

Draft necessary application

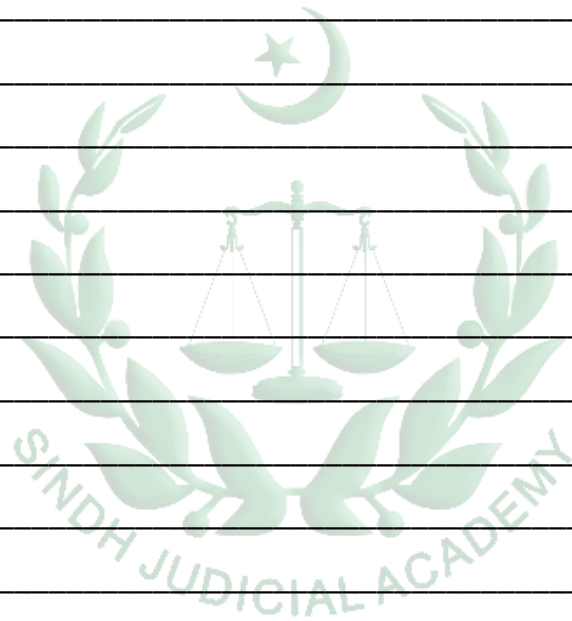


Did you ever approach foreign agency or international organization for the purpose of investigation? If so, how did you approach and what was the information that you requested and its outcome?

Draft letter of request.



What quantum of evidence would be required entitling the complainant for the compensation?




How many help desks are available in your district?

Not established

How many complaints were received from cybercrime headquarter in the last one year?

You have received a complaint for investigation. Complaint reflects two phone numbers from which the complainant received 3 messages regarding

Q. What procedure and steps will be observed to complete investigation?




Sindh Judicial Academy

[illegible]

During investigation you searched a place and accordingly seized a desktop computer, two sims and an external hard disk.

Q. What steps will you take to prove acts of search, seizure and recovery in court of law?

List all possible documents. Prepare all documents necessary in the circumstances.



It is revealed during investigation that one of the directors having 60% share in a Private Ltd Company is Member of National Assembly and part of Cabinet. Data / record shows that he has some business in Australia and UK. He owns properties in UK. In past General Manger of his company was apprehended for the charge of Trafficking but released during enquiry process. He frequently makes call to foreign countries. You suspect that he transferred substantial amount to UK earned from Human Trafficking. You before arresting him need to collect more information and evidence so that his arrest may not be called political victimization.

Q. What action will you take and what type of evidence may be collected and how to collect admissible evidence?

One of the witnesses is reluctant to appear in court to witness an important act as he knows political strength of the accused. He feels danger of life if his name is reflected in final report.

Q. How to treat witness in the circumstances?



