Proposed Amendments in Security Aspects of Draft Broadband Security Policy 2021 Framework for Pakistan, Based on Best Practices Involved in Broadband Security Framework of Contemporary Countries and International Standards

By

Naveed Anjum

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Science and Technology, Rawalpindi in partial fulfillment of the requirements for the degree of MS in Information Security

December 2022

Declaration

I, Naveed Anjum declare that this thesis titled **"Proposed Amendments in Security Aspects of Draft Broadband Security Policy 2021 Framework for Pakistan, Based on Best Practices Involved in Broadband Security Framework of Contemporary Countries and International Standards"** and the work presented in it are my own and has been generated by me as a result of my own original research.

I confirm that:

1. This work was done wholly or mainly while in candidature for a Master of Science degree at NUST.
2. Where any part of this thesis has previously been submitted for a degree of any other qualification at NUST or any other institution, this has been clearly stated.
3. Where I have consulted the published work of others, this is always attributed.
4. Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
5. I have acknowledged all main sources of work.
6. Where the thesis is based on work done by myself jointly with others, I have made a clear exactly what was done by others and what I have contributed myself.

_____

Naveed Anjum,
00000329562

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS Thesis written by **Naveed Anjum**, Registration No. **00000329562** of **Military College of Signals** has been vetted by the undersigned found complete in all aspects as per NUST Statutes/ Regulations/MS policy in free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS degree. It is further certified that necessary amendments as pointed out by GEC members and local evaluators of the scholar have also been incorporated in the said thesis.

Signature: _____

Name of Supervisor: Brig. Dr Imran Rashid

Date: _____

Signature (HOD): _____

Date: _____

Signature (Dean/ Principal): _____

Date: _____

Dedication

“In the name of Allah, the most Beneficent, the most Merciful”

I dedicate this thesis to all my parents, spouse, siblings, Teachers and friends for their unconditional love, endless support and continuous encouragement.

Acknowledgements

All praises to Allah for the strength and His Blessing in completing the thesis.

I am grateful to Allah for giving me strength to complete this thesis, regardless of many problems and issues. All praise to HIM and HIM alone. Next, I am grateful to my whole family and especially to my parents. Without their consistent support and prayers, this thesis would not be possible. I am very grateful to my project supervisor Brig. Dr. Imran Rashid who conducted the work/ research in a very encouraging and helpful way as a supervisor; he facilitated my research, counseled me, he has always been an irreplaceable source of guidance for me and will continue to be in next years of my life. I also thank the committee members who always guided me with their deep and valuable support that helped me in achieving my research goals. Finally I would like to express my appreciation to everyone people who provided valuable support to my studies.

Abstract

Broadband security is an essential component of modern life and a requirement for economic growth, education, health care, and public safety. Maximizing broadband coverage and meaningful use is an imperative for national and individual success. Advances in wired and wireless broadband technology have dramatically changed the way we work, play, and connect with each other. Future proof fiber optics and the next generation of wireless network technology, or 5G, will be transformational. Through forward-looking policy that supports research and development, enables access to spectrum, takes into account security, considers the important role of standards, and provides government incentives and funding to ensure ubiquitous access to connectivity, countries around the world can ensure the successful deployment of broadband and 5G technologies. Following the same level of broadband security requirements other sovereign countries like USA, China, Russia and Malaysia took lead and developed and updated their broadband security framework through coordinated effort amongst business industry and government. This framework comprises of measures, rules, and practices to showcase the safety of imperative foundation.

Broadband security policy of Pakistan was issued by Ministry of Information Technology (MoIT) in 2004 which has become outdated with time. Thus a new broadband security policy is required for furthering the initiative of Digital Pakistan. It is pivotal to craft a policy vision that is user-centric, market-oriented, simple to govern, and all-inclusive, laying a strong foundation to address outstanding issues expediently and explore new opportunities in the most agile manner.

This broadband security framework will provide a general perspective on all components of digital development and broadband security that need to be considered by ministries and Government agencies in digitizing information. Accordingly, the ministries and agencies of Pakistan will develop their respective Department's broadband policies based on this framework and the Public Sector broadband security Policy to manage and ensure that all activities carried out in the Department comply with the requirements highlighted.

Table of Contents

List of Figures

List of Tables

Chapter - 1

Introduction

World's total economy and defense of countries can be placed at risk due to data breaches and broadband network security failures. Each crime **committed** in **broadband** domain shreds trust and senses of security of public as malicious factors have **demonstrated** their **ability** to commit crimes even in **securely governed systems**.

A great deal of resources is invested to secure the national critical infrastructure. Cybercrimes which are generated due to breaches of broadband network needs to be addressed with complete dedication and professionalism. This require a great deed for formulation of broadband security policy formulation its implementation in true letter and spirit. "The art of war" is an ever-changing phenomenon and a process as to how, when, and where to engage the enemy. Globally a relatively newer threat is evolving not only for states but also for the private profit driven world. Billions of dollars are illegally transferred or stolen, privacies exposed, state secrets acquired, and critical public infrastructure hacked. This is the realm of broadband infrastructure security. As the world becomes more and more connected via internet or digitized through information technology, the cyber security threats are increasing day by day.

Several countries have devised and enacted initiatives in broadband domain, for example: United Kingdom has enacted **"Online Security Bill"** to look after for digital broadband services and bars any malicious, illegal and harmful activity. Comprehensive broadband security frameworks of **United States of America**, **India**, **Malaysia**, **Qatar**, **China** and **United Arab Emirates** are given in figure below for a quick overview.

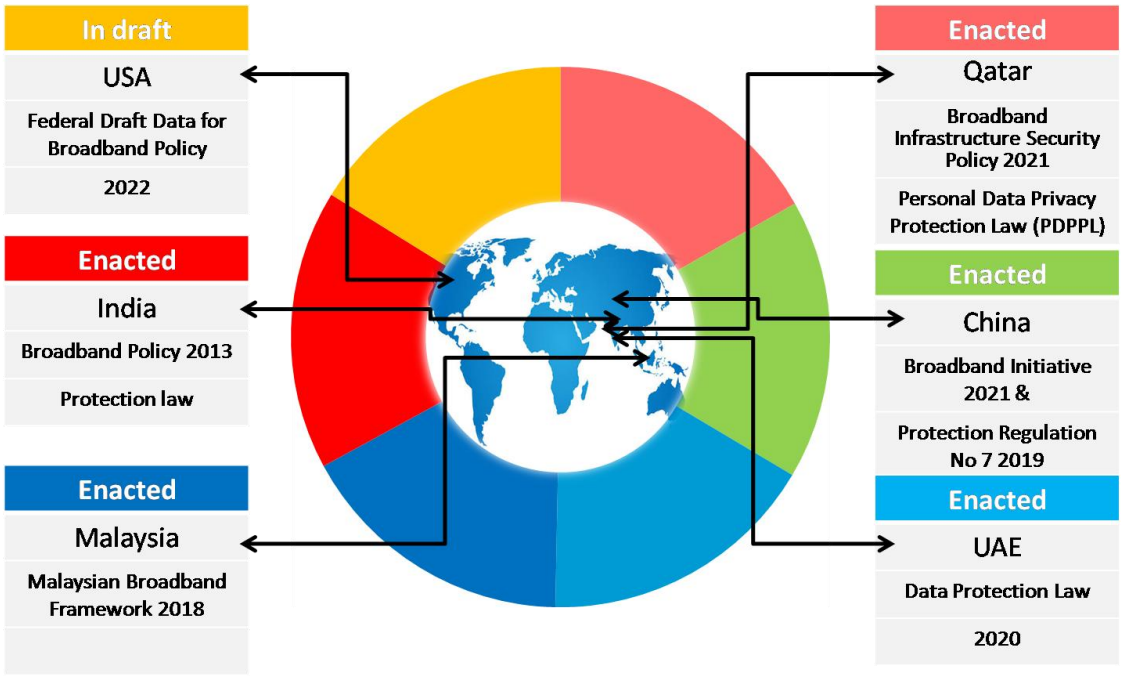

Fig-1.1 Broadband Initiatives in the World

The advent of **5G communication** has bloomed the broadband connectivity and reshaped it in a novel manner and soon operators will be able to design and deploy a **software-defined** and virtualized infrastructure in almost all domains of life which will solely work on fast computing and broadband network connectivity. Although the evolution of networks brings along security features too, still there is need of a separate **robust broadband policy** that govern the **safety** and **security** of both the **users** and **operators** and provide them with a safe and **secure broadband environment**.

1.1 Problem Statement

MoITT has issued the **Draft Broadband policy-2021** but security aspects have not been covered. The broadband ecosystem has the opportunity to play a positive role in society and economies, strengthening infrastructure, institutions, and systems that not only address the current challenges posed to Pakistan by the **COVID-19 pandemic (Online Study, Online Work from home, Tele medicine, e-commerce),** but also prepare the world for future disasters in world and specially in

Pakistan. Therefore, the need to maximize for the global broadband community and partners to maximize its potential positive contributions to the digital economy of Pakistan is significant and cannot be overstated. Building back better with broadband, preparing against future shocks, and ensuring universal equitable access is part of the new normal will require an emphasis on digital infrastructure and technologies in the pandemic response, recovery, and resiliency-building efforts. In this perspective, **this study analyzes broadband framework of contemporary countries and international standards and proposes broadband Framework of Pakistan by incorporating best practices involved**.

1.2 Objectives

The main objectives of this thesis are:

- Analyzing already implemented broadband Frameworks in contemporary countries including **China, USA** and **Malaysia**,
- Analyzing **International Telecommunication Union (ITU)**broadband Framework for international standards,
- Proposing high-level perspective of **Broadband Security Framework for Pakistan** incorporating best practices involved.
- To address the demand for affordable access to **broadband for everyone**,
- To address the **challenges regarding the digital divide,** particularly in un-served and underserved areas nationwide,
- Overcoming the difficulties in rolling out the required digital infrastructure and related investment models,
- Harmonization of **existing tax regime on telecommunication services**,
- Encouraging the development of **local and relevant content and services**,
- The need for upgraded and consistent broadband quality of service,

- Promoting the importance of **digital trust over telecommunication networks** to use digital technologies in all fields of life,
- To understand the impact of the **internet on socio-cultural progress, economic growth,** and environmental sustainability,
- **Reducing barriers for investments** applied on existing licensees and new investors in the telecom sector and promoting public-private partnerships,
- **Adoption of Xth Generation technologies** for improving the state of broadband infrastructure, and
- **Security of broadband network**.

1.3 Relevance to National Needs

As all most of the departments in Pakistan have turned digital and need online internet system for connectivity, therefore there is dire need to formulate a comprehensive broadband policy.

Officially Pakistan has the broadband policy but it lacks in many aspects which need updating the policy. This research work will propose a high-level description of broadband framework that shall be used by ministries and agencies in Government and Public Sector to plan the necessary protection for their respective cyberspace.

1.4 Advantages

The impacts of proposed framework will be to:

- Provide a more effective and comprehensive broadband policy,
- Ensure the smooth functioning of existing Government digital services, and
- Increase stakeholders' confidence.

1.5 Delimitations

Proposed National Broadband Policy will deal with security of broadband world and information technology users along with **elimination** and **reduction** of **crimes**

related to it on **nationwide level**. **Crimes** and **malpractices** are ever increasing and **mustering** on **daily basis** and each day brings a **new noose threw by criminals** of cyber world. This policy will bring **laws** and **regulations pertaining** to the **broadband domain** and its **subordinate framework**.

1.6 Areas of Application

- Government and Private Organizations using Information and Communication Technologies (ICT) services,
- IT Industry,
- Telecom Industry,
- Transport Industry,
- Banking Sector,
- Health Industry,
- Education department, and
- E-commerce industry.

Chapter - 2

Literature Review

Pakistan bears a large internet based user community. With each passing day, the user's toll is increasing. Every public and private sector like banking, health departments, aviation etc has switched to the **digital world** and **heavily relies** on **internet connectivity**. Pakistan is facing **severe cyber threats** amid its **location** and **nuclear** status. Although there are laws and legislation which counter the crimes of digital world; yet these are not enough as new threats and malicious vectors are emerging as the technology proceeds. In this regard, **National Broadband security Policy [NBBSP V1.0]** is being formulated and is incorporated with cyber crime laws to deal with threats **emanating** in **broadband world**.

The literature studies for this work are to review the **enactment**, **domains** where these policies are implied and area where these policies fail to address the problem rose **worldwide**. Further, legislations and cyber crime acts which have been implemented in Pakistan are reviewed so a new component for the proposed **National Broadband Policy** is formulated.

2.1 Malaysian Broadband Framework

First version of **Malaysian Broadband Framework** was developed in **April**, **2016**. This framework further enabled the **ministries**, **agencies**, and **public sectors** of **Malaysia** to further develop their broadband policies based on said framework. This policy ensured that all the **cyber activities** carried out in Malaysia must comply with it.

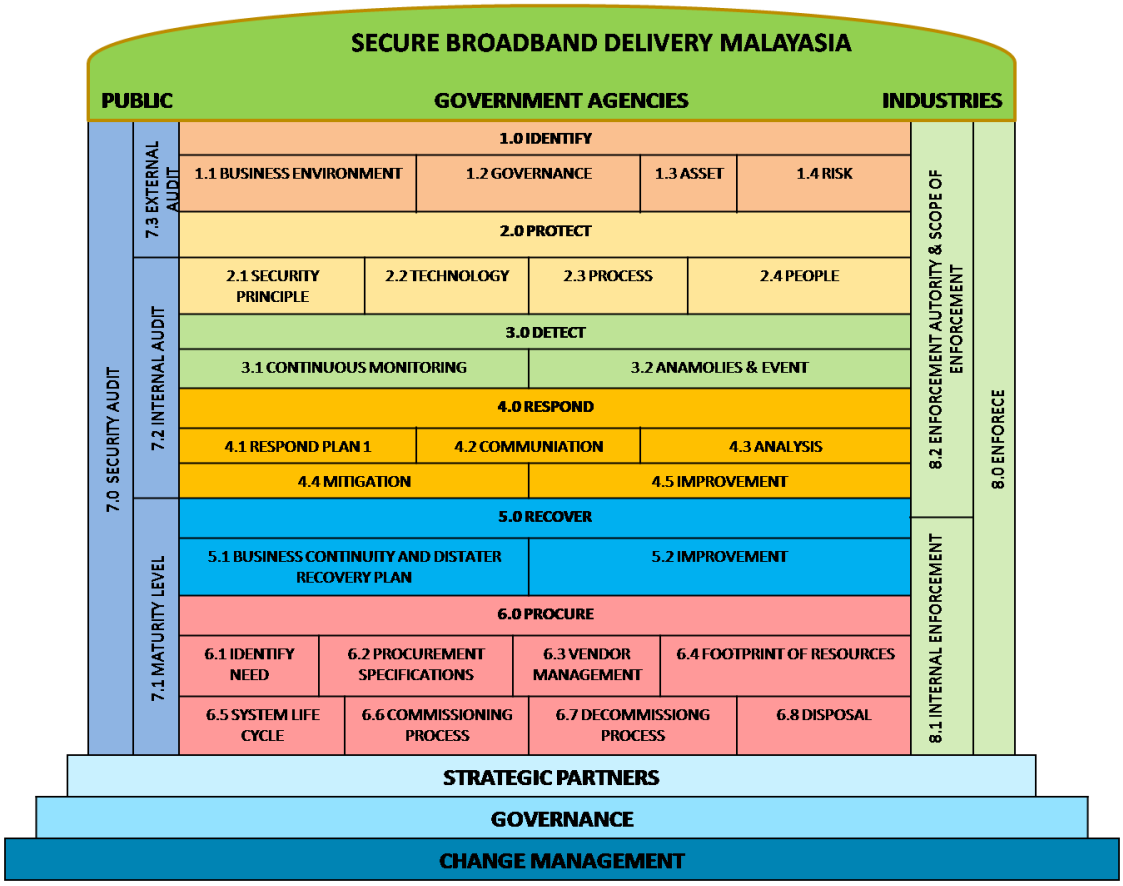

Figure-2.1: Malaysian Broadband Framework (MBF)

The framework of Malaysian Broadband Policy consist **eight major components** whose functioning is briefly described below:

- **Identify**: Identification component of this policy focuses on the functioning environment, policies that govern the department, structure and assets that needs protection, **identification** of **risk** and **subsequent risk management**.
- **Protect**: This component deals with the principal of technology, safety, process and human ability to determine the **mitigation level** of **identified threats**.

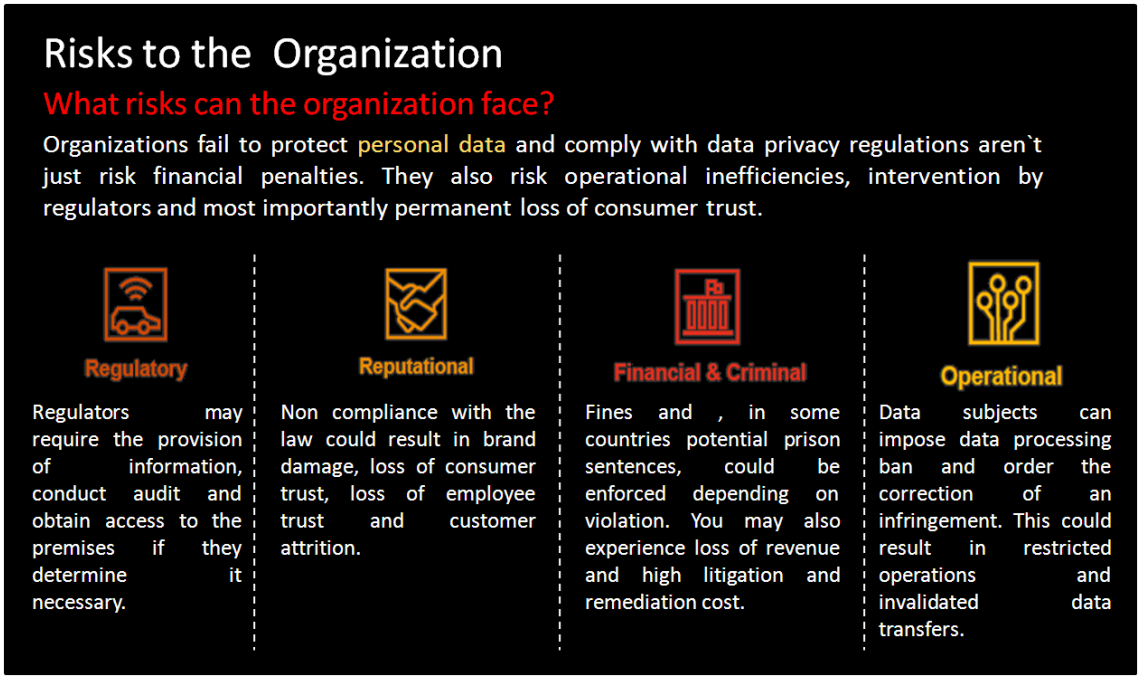

Figure-2.2: Risks to the Organizaiton

- **Detect**:Detection of malicious and **unauthorized activities** are carried out in this phase. For example detection of any exception of block of software code is done here.
- **Respond**: This step deals with the actions carried out to **mitigate** the **identified malicious activity**. Intimation to the administrators, users and stakeholders are also informed.
- **Recover**: **Recovery** of any **damage** sustained due to malicious activity is carried out in this step.
- **Procure**: Procure step deals with the **security controls**, development life cycle and **procurements** for **system**. Supplier company management and procurement specifications are also dealt by this entity.
- **Security Audit**: Security audit of **all components** of **system** concerned is carried out under this domain.

- **Enforce**: This section implements and enforces laws and regulations which are recommended by the **audit agency** and concerned **enforcement authorities**.

An important feature of this component is that is also defines **procedure** for **handling** of **Official Confidential Information** and active **role** of **Chief Security Officer** for the creation, handling, storage, classification and disposal of official information. Key aspect of **Malaysian Broadband Security Framework** is that it ensures implementation of appropriate safety principles on right time along with risk assessment and management. This policy covers threats emanating from technological grounds and cyber related content. Core objective of Malaysian Broadband Security Policy was to alleviate the risks and counter threats to **Malaysia`s critical information infrastructure** and their **protection**.

CYBER THREATS

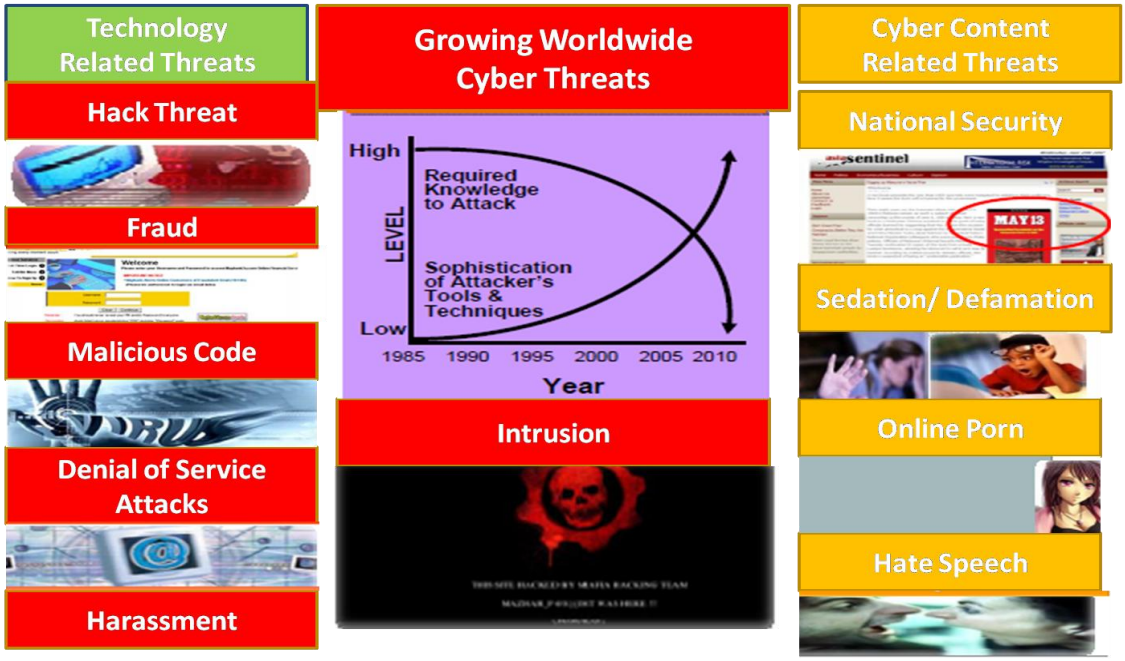

Figure-2.3: Malaysian Broadband Policy and Cyber Threats

Figure-2.4: Malaysian National Broadband Policy Framework

Legislative and Regulatory framework of Malaysian Broadband Policy comes under **Policy Thrusts – 2** and enables **Attorney General** to abate in cyber crimes threat

and increase in security by applying **legislative and regulatory framework** in appropriate manner.

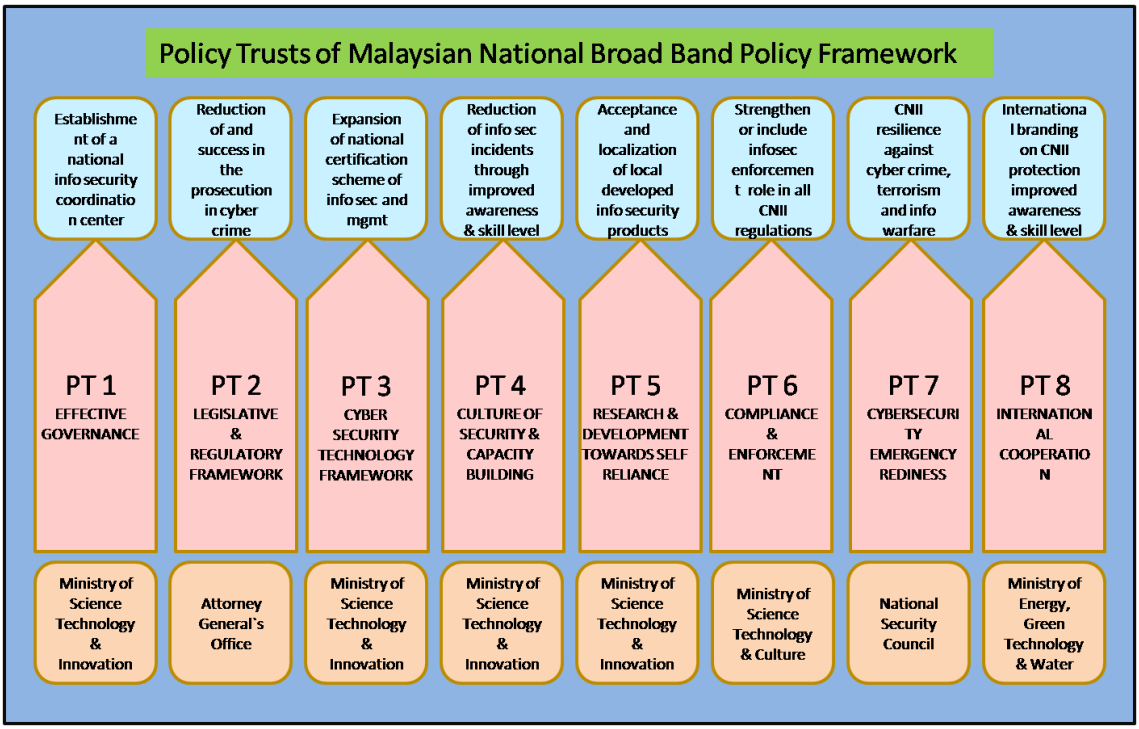

Figure-2.5: Policy Trusts of Malaysian National Broadband Policy Framework

National Broadband Policy of Malaysia was implemented in **three phases** and implementation goals were set to be achieved in **time frame of year 1 to year 5**. Governance body consists of:

- IT Council,
- Advisory Committee,
- Coordination Committee, and
- Working Group.

Committee formed for the **Regulatory** and **Legislative Framework** studies laws of Malaysia to accommodate and adapt the legal hurdles in broadband world. The committee has following three main agendas:

- To identified the challenges, issues and difficulties regarding internet.

- To further develop the **legislative framework** which will counter the conventional as well as **cyber specific threats**, and
- To oversee the recommendations and amendments required in current broadband framework. There will be also efforts done by the committee to look after the process of **harmonization** and **reconciliation** the **legislation** with the **current legislation**.

2.2 Chinese Broadband Framework

The main point of **China`s Broadband Policy** is to **enhance** the **data confidentiality**. Implemented in June 2017, key emphasis was laid on improvement of national broadband world level. Key infrastructure (both **civil & military**), personal information and network were main domains where implementation of security and classified protection were implied. Also, **Broadband awareness**, cyber related emergency management, violation of broadband policy laws and subsequent punishments, security responsibilities and personnel training in broadband area were applied.

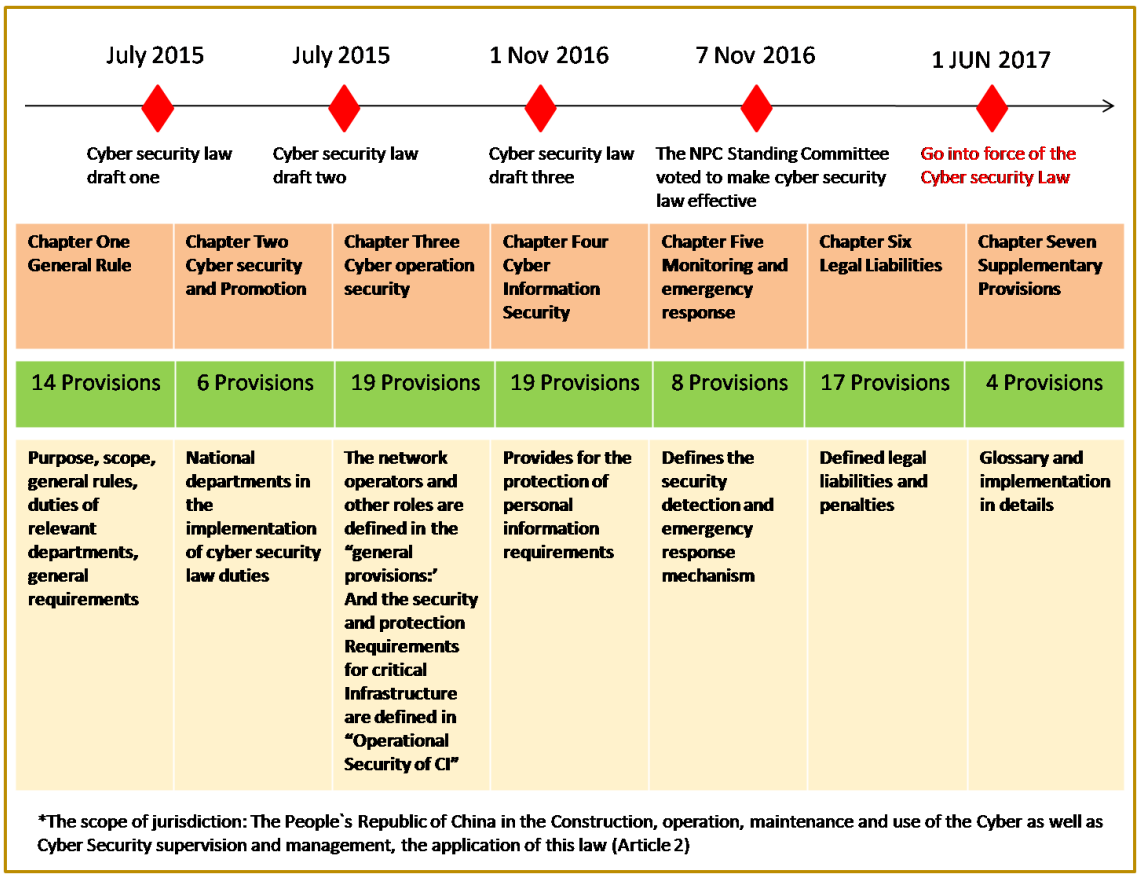

Figure-2.6: Chinese Broadband Law Framework

Further work on implementation of added security regulation of classified systems, **Critical Infrastructure protection** requirements, **transfer** of **data across border** and **certification** of certain network is being carried out.

This policy was the very first of its nature in China and it created a novel regime and stage for **China`s Broadband Administration**. It also devised **punishments** to the **violators** of **policy laws**. Chinese Broadband Policy generally covered the operations, maintenance, construction of **any network** within **China`s territorial boundaries**. The major protection requirements for Chinese Broadband Policy include:

- China based **storage** of **important data** and **personal information**,
- Performing **Security assessment** for **cross border transfer of data**,
- Review of National security requirement on **reliability** and **security**,

- Laws and regulations regarding **cybercrime** or **data breach**,
- Protection measures at **organizational** and **technical level**,
- **Maintenance** and operation of **critical information infrastructure** (CII),
- **Scrutiny** and **security testing** of **out sourced vendor software**.

In China`s Broadband policy, most **significant** and **important emphasis** is laid over **data transfer across border**. Data localization and security assessment requirement are necessary for operators for data localization. Following figure defines **twenty-eight (28)** significant **data export guidelines for industrial sectors**.

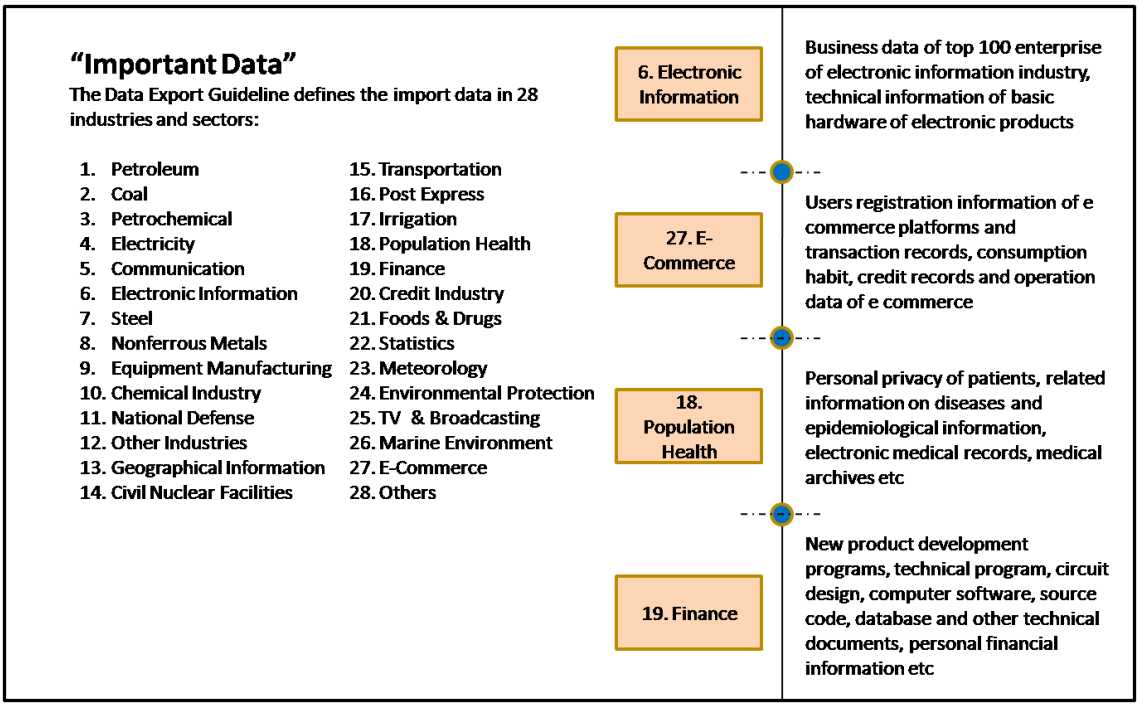

Figure-2.7: Data Export Guidelines

Strict penalties in case of non-adherence to the policy are also introduced. Following order of penalties are devised from low to severe level of non-compliance at company level:

- **Office order** for **making correction**,
- **Verbal** & **written warning**,

- **Deprivation** from **legal gains**,
- **Suspension** of **business**,
- **Closure** of **website**, and
- **Suspension** of **business permit/ license**.

Following order of penalties are devised from low to severe level of non-compliance at individual level:

- **Trial** and **imprisonment** under criminal law,
- **Detention**,
- **Public Surveillance**,
- **Removal** from **key position**, and
- **Fine**.

Chinese Broadband Law compliance was compared with **GDPR** on aspects of **interconnectedness** and **compatibility**. Following points were observed **during analysis** of **both policies**:

GDPR	Chinese Broadband Law
Focuses only on personal data protection	Emphasis both on Protection of Personal data and Broadband & Critical Information Infrastructure protection
Requirements on personal data protection are cumbersome	Requirements of personal data protection are comparatively lenient
GDPR has clear rules regarding data transfer	Chinese Broadband Law has ambiguous and unclear assessment standards

2.3 Russian Broadband Framework

Russian Broadband Security Framework was enacted in April, 2016. This policy covers legal, organizational and technical measures, corporation, capacity building and child protection. Chief aspects covered in Russian Broadband Security Framework are given below:

- **Legal Measures**: This section of the policy deals specifically with the extension of **Instrument of Criminal Code in criminal legislation process** on **broadband domain crime**. Several other instruments meant to contain and stop spam, individual information, protection of legal entity, legislative regulations and technical matters.
- **Technical Measures**: In order to **detect** and **suppress illegal activities** related to **broadband networks of Russian** government bodies, Russia has developed Cyber Incident Response Team (CIRT) in information systems of its government authorities. This policy contains standards in compliance with internationally **recognized broadband standards**.
- **Organizational Measures**: **"Basic Principles for State Policy 2020"** was adopted officially by Russia in field of International Security. This law enforced all government departments of Russia to perform an **annual self audit** of organizations owned broadband networks and installed systems.
- **Capacity Building**: Russian Federation has set **multiple Research** and **Development** programs in field of broadband networking in national universities. Universities have been assigned to **train the professionals** in broadband network domain.
- **Cooperation**: Sharing of critical data and cooperation in broadband domain with neighboring countries is covered under CIRT. Comprehensive framework has been set to facilitate the sharing of information. **Federal Security Service (FSB) of Russian is responsible for exchange of information at international level**.
- **Child Online Protection**: Special care has been taken on formulation of policies regarding **child protection** in **broadband world**. Any content or information which may **proof harmful** to children or their health is **strictly forbidden**. Russian Broadband Framework incorporates laws

and regulations to assure **Digital Sovereignty of Russia**. This portion of broadband framework has following key components:

- **Data Localization** Law,
- **Legislation** of **Imports** Law,
- **Critical Infrastructure Law**, and
- **State Owned Cooperation**.

2.4 USA Broadband Framework

Current president of USA, Joe Biden promised during his presidential campaign to boost the broadband structure of America`s 5G network and expanding it to the reach of every American national. Joe Biden further gave idea of "**Universal Broadband**" by announcing "**Bipartisan Agreement for a Large Infrastructure**" bill.

Broadband gained more importance in USA that it had ever before. Due to COVID-19, 7.2% household connections have upgraded their broadband network connection. This should be noted that 41% of US households have attended the school or worked from home during pandemic outbreak.

- **Structure of USA Broadband Network:** Structure of **USA** Broadband network is **highly dependent** on private ventures. Telecommunication carriers, wireless ISPs, cable service providers and other related broadband structures run on private investment. All sorts of users avail these services thus **very strict and robust broadband policies** are followed and these are favored by users.
- **Subsidy for Un-served or Under-served Markets:** Access of **high speed broadband network** to users in **underserved** and **un-served markets** of **USA**, due to difficult geographical location or other reasons is countered by subsidies given by FCC and other federal agencies. Earlier the networks for providing network connections was based Public Switched Telephone Networks (PSTN) but now these are switched to broadband connections. This switching has in turn has proved vital to the

domains of tele-health applications, remote learning/ e-learning and expansion in business networks. **Biden Administration** has poised to invest **$65Billion** further in broadband infrastructures providing network to un-served and underserved areas of **USA**.

- **Service Affordability Offering:** Exclusive programs run by USA government during COVID-19 gave generous subsidy and discounts for household broad band connections. **"Emergency Broadband Benefit (EBB)"** scheme has offered a discount of 50 Dollar per month in household broadband connection and discount of $100 (one time) for purchase of broadband internet device. This scheme resulted in enrolment of more than 6.1 million households as late September, 2021. Along with this, **$7.17 Billion** are sanctioned in **"Emergency Connectivity Fund"** through which financial support will be given to libraries and schools to equip their labs with laptops, pads and tablet computers so to facilitate residents of communities and students **in accessing broadband internet**.
- **Security of Broadband Networks:** Bloom in broadband connection and networks has brought with it **dangers** of **hacking** and likewise **security threats** too. **USA** is more concerned over potential threats to national security posed from communication infrastructure and devices of foreign origin. This concern lead to the ban on equipment of **ZTE** and **Huawei Corporation** and further **removal** of **pre installed devices** of **Chinese origin** companies from telephone networks by Donald Trump`s Administration Executive Order on **"Securing the Informational and Communications Technology and Services Supply Chain"**. Another Act "Enactment of the Secure and Trusted Communication Network Act, March 2020" has boosted the working pace of FCC too. **"Third Future Notice of Proposed Rulemaking"** was forwarded by FCC in 2021 to

augment the **"Rip & Replace"** process. This rule finally became the **Formal FCC Rule** in **July 2021.** Under the umbrella of said rule, intense working was carried out in upcoming 6 months to finalize an initial list of **"devices, equipment and services"** which posed immediate threat to National Security of USA. Further to compensate and reimburse the affected entities by "Rip & Replace" program, FCC initiated **"Secure and Trusted Communications Network Act March-2020",** administered by **Ernest & Young, LLP**. Through this program, funds were sanctioned to reimburse the affected entities to cover the cost of their communication items **impaired** by **rip** and **replace program**.

- **Way Forward:** **United States** of **America** possesses very divers, dynamic and complex infrastructure of broadband networks. No matter how secure their networks are and how much accessible their network is to their people, **broadband development** shall always be **backed** by **strict broadband regulations** and policies in order to provide a secure, fast and affordable broadband service to **USA residents**.

2.5 Critical Telecom Data and Infrastructure Security Regulations-2020

Pakistan Telecommunication Authority (PTA) forwarded **"Critical Telecom Data and Infrastructure Security Regulations Act, 2020"** for secure handling of critical data and its infrastructure in telecommunication sector. These both entities will be designated and identified by **Pakistan Telecommunication Authority (PTA)`s** license holder to ensure broadband security. Automatic network monitoring will be implied to detect and counter any **unauthorized** or **malicious user(s), connection attempts**, **device attachment** and **software interference** with **preventive actions**.

- **Critical Telecom Data and Infrastructure Security Regulations:** Critical Telecom Data Infrastructure (CTI) will constantly be **monitored** by the **authorities** to identify and bar any attempt of malicious activity including **unauthorized access**, **eavesdropping** on **communications**,

and other **broadband threats**. These regulations are made to implement the powers given by **Clause-0; Sub-section-(2); Section-5;** of the **Pakistan Telecommunication (Reorganization) Act, 1996 (XVII of 1996)**. Further, broadband world security awareness will be disseminated by the license holder with the other partners & entities through lectures, trainings, awareness sessions and complementary trainings.

- **Physical Security of Secured Areas:** It will be the responsibility of the license holder to designate the secure areas and **implement its physical security** and further to make it sure that access to secure area should only be **limited** to **authorized persons** and maintain the log of access. License holder will make it sure too that in case of any mishap, the effected system may instantly be **isolated** from **core of Critical Telecom Infrastructure (CTI)**. License holder will make it sure to provide physical security to the secured area from:
  - **Natural Disasters**,
  - **Hazards**,
  - **Malicious Attacks**,
  - **Electronic Interference**,
  - **Incidents**, and
  - **Power Failures**.
- **Aspects of Hardware Security:** In order to carry out **repair** and **maintenance** of equipment installed in secure area, only authorized service person will carry out the repair work and all other **unattended hardware** has to be **safeguarded** from any **unauthorized access**. Any hardware system linked to or part of **CTI will not be taken off site** and **out** of secure area premises without proper permission. License holder will ensure the following event logs w.r.t hardware security:
  - **User Activation**,

- **Exceptions**,
- **Fault Occurring**,
- **Cyber Incidents**, and
- **Threats**.

- **Aspects of Software Security:** The software domain of CTI systems will be **thoroughly** and **regularly inspected** by License holder and will be responsible for:
  - **Elimination** of **malicious software activity**,
  - **Use** of **unauthorized software**,
  - **Prevent installation** of **unlicensed software**,
  - **Data** & **software backup** in case of **malware attack**,
  - **Prevent unintended use** of **software**,
  - **Protection** of **data** from **loss**, **modification**, **unauthorized disclosure** and **destruction**, and
  - **Obtaining** of **software** from **trusted vendors only**.

2.6 Personal Data Protection Bill-2021

Personal Data Protection Bill 2021 is enacted to govern the process of collection, possession, use, processing and disclosing of personal data and about offenses pertaining to the violation of the data privacy right by any means.

Personal Data Processing and Obligations of the Data Processor & Controller:

The assortment, processing and disclosure of customer`s personal data entities must be done only during acute needs and must not be used in incompatible purposes. This **personal data must** be **processed** in **lawful way** and **under supervision** of data controller. This collected/ processed personal data must not be disclosed without personal will/ approval of the data subject.

Collected data`s security is regarded very crucial and international standards must be followed/ adhered to protect this data from suffering any loss, modification, un-intended use, accidental or unauthorized access, alteration or/ and destruction. The

data must not be kept after fulfillment of task for which the data was obtained. However **data controller** is advised to keep and maintain a record of each notice, application, and request of information which were processed by the **data controller**.

In case of any **data breach** to personal data repository, data controller must inform the authority **not more than 72 hours of delay**. Data controller too has to keep the record of personal data breaches, its effects and actions taken in this regard.

Rights of Data Subject

This clause **allows user to access his/ her personal data** by **paying** the **administrative cost** and **producing written request** to the **data controller**. Data controller has to maintain a formal consent of sharing data with the data subject. However the data controller can refuse to produce the information to the data subject and if it is felt that key/ necessary verification information is false, misleading, obsolete or conspicuous and the data subject can-not be identified from the information provided.

Correction to this **personal data** can be made only after **pleading a formal request** and **producing actual data**. Data controller will make it sure that data provided by the entity for correction is accurate and valid, if the data controller is not provided with the sufficient and accurate information, data controller has the right to refuse the updating request. This act has given data subject the rights for erasure of personal data and **data controller(s) must has/ have to comply** with the request within **fourteen (14) days.**

Sensitive Personal Data Processing

Data controller is not authorized to keep the sensitive personal data of any data subject(s) unless his/ her personal approval for the personal data processing.

Exemptions

Collection of data by data controller from the data subject is termed as **"First Collection"**. **Personal data may only be processed** by data subject only for the purpose of data subject`s personal, household, recreational or family affairs purposes must be **let off** from clauses/ **provisions** of said act.

The Commission

After passing six months of enactment of this law, Federal Government shall establish a commission which will be called **National Commission for Personal Data Protection (NCPDP)** of Pakistan. This commission will be a statutory body, and will possess a common official seal. Further this commission is allowed to establish its sub offices in provincial capitals. The commission will be fully responsible for safeguarding **personal data** of data subjects and will **prevent data misuse**, promote awareness and will entertain complaints under this act. Commission will consist of five members and with having **following expertise**:

- An Information and Computer Technology (ICT) expert,
- A Strategic Interest Expert,
- A Legal Expert,
- A Representative of Civil Society, and
- A Financial/ Accounting Expert.

Complaint and Offences

According to this act, anyone who is involved processes, causes to be process, discloses or disseminates the personal data, will be **punished** with **upto 15 million rupees** and if involved in **unlawful/ unauthorized personal data processing**, the fine amount may be **increased** to **PKR 25 million**. The data controller **who does not** to adhere to the necessary security/ precautionary measures for data security shall be fined up to **PKR 5 million**. Anyone who does not comply with the orders/ laws of commission is liable to be fined upto **2.5 million rupees**.

Any data subject or concerned individual can file a **complaint** to the **commission against violation of personal data protection law**, misbehave or conduct of data controller or data processor in case of breach in personal data of data subject`s or in performance of data processor. **Appeal against** the commission`s **decisions** will be referred to the **high court** or any **tribunal** within **three months**.

2.7 Prevention of Electronic Crime Act (PECA) – 2016

Advancement in technology and broadband communication has brought along novel cyber crimes too. To cope up with this problem, government institutions are constantly working to formulate new laws. On advice of National Action Plan (NAP) Committee, **Prevention of Electronic Crime Act (PECA)** was formulated to nab anti-terrorism agenda of the nation.

PECA is a very comprehensive law which covers all sorts of electronic and digital crimes committed at national level. Although some Non-Governmental Organizations (NGOs) raised concern over PECA`s enactment as it will severely hamper the **"Freedom of Speech"**, yet it gave **additional powers** to **government agencies**; for example to **Federal Investigation Agency (FIA)**. PECA deals with the all stages in addressing of cyber related crimes.

All **offences** are regarded **cognizable** except **sexual harassment**, **sexual blackmailing**, **revenge porn** and **pedophile** / **child abuse**. Theft of credit card credentials and money laundering are also not included in cognizable offences.

PECA can be implemented in its true essence if and only if local **courts do not interfere and hamper the working methodology/ system** of law enforcement agencies, without doing so the law enforcement agencies will not be able to counter threats as per citizen`s requirement. In **PECA**, **Section 37 empowers Pakistan Telecommunication Authority** to block or remove any **unlawful data**. But it provides no definition of "unlawful", thus creating ambiguity in discrimination of vast amount of data.

2.8 Prevention of Electronic Crimes Ordnance – 2007

This ordnance was formulated to **preserve** the **integrity**, **confidentiality**, **integrity** and **availability** of **sensitive information** and data as per definitions of government of Pakistan and her law and enforcement agencies. According to this law, **imprisonment of 2 years (minimum)** was approved against criminal access of data or damage to data. **Attempt** to **breach** in **data** was too considered **crime** under this act.

Minimum **imprisonment** of **7 years** was devised on committing of electronic frauds, forgery, cyber stalking and use of malicious software codes.

Although comprehensive, yet this ordnance lacks coverage and punishments for several novel crimes; for example frauds in credit card transactions.

2.9 Telecommunication Consumer Protection (Amendments) Regulations (TCPR) – 2016

This regulation (amendment) covers all kinds of commercial practices, including **Telecommunication Services Promotional Schemes** being offered by an operator. This act also describes that promotional schemes contrary to law shall not be launched by an operator. Operators are openly allowed to offer its customers incentives for service promotional schemes. These incentives shall include **concessional rates** and other incentives. Any proposed commercial activity must be reported by the operator to the Authority at least **ten days earlier**. In this regard, copy of promotional scheme, charges and rates must be provided to the Authority. The proposal for information provided by an operator be clear in all respects, transparent and having no discrimination.

This regulation also binds the operator that it shall not send any unsolicited message or **Interactive Voice Response (IVR)** broadcast unless it is requested/ subscribed by the consumer. While **promoting** any **commercial practice** or **activity**, operator will make it sure that any **textual information must be easily readable** and **understandable**, and be presented in **horizontal way**. If the promotional stuff is produced in video or audio format, its duration and other visual details must be presented. In case of qualifying a **contest** or any **game show**, the details of **winner** must not be **disseminated without consent** of the **winner**.

Promotional and all other activities related to **Telecommunication Service** promotional schemes do declare a disclaimer to general public to stay aware of malicious and fraudulent schemes on behalf of the operator and demand for transfer of

money/ credit against schemes. Along with that, all operators are liable to keep **complete record** of **commercial practices/ activities** of **last five years**.

2.10 Telecommunication Consumer Protection Regulations (TCPR) – 2009

These regulations imposed by Government of Pakistan in April 2009; covers the **Service Provisioning**, **Interruption** and **Disconnection** of services to the telecommunication users. This law, allows users to opt the service provider of his choice, and further notifies that services must be provided to the users (customers) in **transparent**, **fair**, **non-discriminatory** and in **efficient way**. According to this policy, any change, expansion, upgrade or activities pertaining to the service or network must be notified thirty (30) days prior imposing of changes and all the unforeseen interruptions caused by either technical or non technical issue must be **conveyed** to the **customers** in **shortest possible time.** Also operator can **withdraw** the services to the **user thirty days prior notice** to the user.

- **Commercial Practices:** This provision restricts that the **operator** shall **not use unfair Commercial Practices** when selling services to the customers. Any information which is hidden, omitted, production in an unclear method or unintelligible will be regarded as **misleading omission**.
- **Code of Commercial Practice and Service Contracts:** All operators, who want to take approval from the Authority concerned regarding Commercial Practice Code, they must publish their standard **contract** of **service** and code of **commercial practice**.
- **Nature of Complaints:** All operators are to provide positive response and to entertain the complaints lodged by customers. However following nature of **complaints have exception**:
    - **Misuse** & **Quality of Service**,
    - **Involvement** in **Illegal Practices**,
    - **Poor Services**,

- **Misleading Statements**,
- **Non Provision** of **Services**, and
- **Complaints** regarding **Mobile Number Portability**.

- **Confidentiality of Information:** All working staff of operators must maintain strict confidentiality regarding **information** and **details** of their **customers** and will make it sure this **information must not leak** to any **third party in any case**.
- **Publication of Consumer`s Manual:** All operators shall publish and maintain consumer`s manual and advertise it using print or electronic media **not late that ninety (90) days** of **imposing** of these regulations. The manual must contain the following:
  - **Customer`s services helpline**,
  - **Pre-requisites** in **obtaining** of **new connection**,
  - **Tariff, charges** and their **application**,
  - **Standards** of **quality service**, and
  - **Methodology** of **resolving complaints**.
- **Force Majeure:** Circumstances beyond the real and reasonable control of **operator**, **acts** of **God**, **Civil disorder**, **insurrection**, **war** or **military operations**, **emergency** (local or national), **flooding**, **disputes**, **weather** or **exceptional severity** for which the operator is not responsible, the operator shall not be regarded **responsible** and **accountable** for that period to a customer with **respect to any service**.

Chapter - 3

Broadband Policy Framework

3.1 Introduction

The role of broadband infrastructure policy is of very crucial importance in all domains of a particular country. With the sophistication in computer, networking and information technology infrastructures; attacks on these entities have also risen at dramatic level. To maintain the vitality, integrity and quality of the network and services of broadband network, comprehensive policy is very important.

3.2 Aim

The main aim of this policy security framework is to provide controls in order to ensure that Pakistan`s broadband infrastructure must meet the requirements of her community at large and to provide service providers with clear and unambiguous guidelines on the expectations the users will have from them.

3.3 Scope

This National Broadband Security policy framework shall be applicable to:

- Internet Service Providers (ISP) of Pakistan,
- Broadband infrastructure of "FTTH" and "Hosting Websites",
- Hosting Providers in Pakistan.
- National DNS & ccTLDs functions and MoITT of Pakistan,
- Users/ Consumers

3.4 Internet Service Provider Infrastructure Security

3.4.1 Internet Service Providers (ISPs) will ensure that components and design of broadband internet infrastructure network and its associated technology are adopting and adhering to the best practices recommended by the vendors for security, high availability and recovery of data.

3.4.2 It will be the responsibility of Internet Service Providers (ISPs) to comply with product security controls mentioned in National Broadband

Policy [NBSP V1.0] and put forward independent evaluation and security requirements for vetting for core components of broadband network infrastructures like routers, core switches, internet gateways and authoritative domain name servers (DNS).

3.4.3 Internet Service Provider shall ensure the application of cryptographic security controls at entities where these are technically feasible. ISP will too responsible for hardening of broadband network backbone equipment like routers, core switches, internet gateways and authoritative domain name servers (DNS) as per international and vendor specific standards.

3.4.4 Internet Service Provider shall ensure the diversification of core broadband networking infrastructure by adopting technologies from multiple vendors and must refrain from "Vendor Lock-in" wherever possible.

3.4.5 Internet Service Provider will maintain and manage, with applying best practices for complete and round the clock monitoring of system, change management and logging of broadband internet infrastructure.

3.4.6 Internet Service Provider will ensure that any access to the broadband infrastructure used for broadband internet from outside Pakistan must be strictly monitored and complete log be prepared of this.

3.4.7 Internet Service Provider will ensure the use of detection and prevention technologies in order to protect the customers as much as possible from malicious attacks, for example Botnet activities and DDoS attacks.

3.4.8 Internet Service Provider will ensure that broadband home appliances provisioned by it to user are hardened according to the best practices and standards of that time and these devices must not contain any backdoor which may result in customer`s privacy breach.

3.5 Broadband Routing Security

Internet Service Provider will ensure to implement authenticated external Border Gateway Protocol (BGPs) sessions, supported by technically partner peers. Authentication for internal Border Gateway Protocol (BGPs) session shall also be employed. International and national peering to ensure the integrity of internet feed to the consumers and there must never occurs even a single physical or logical failure.

3.6 Domain Name Services (DNS)

Internet Service Providers, Country Code TLDs (ccTLDs), sponsored as well as unsponsored, Generic TLDs (gTLDs) server owners and Ministry of Information Technology of Pakistan, all must ensure that:

- There must not occur any single point of failure,
- Strict forbidding on remote access must be maintained and Management & administration rights must be reserved,
- Enforcement of robust policies of password and its implementation on core components of broadband internet infrastructure in strict accordance with NBSP [V1.0],
- System access must be maintained and last six months log data must be kept,
- Use of secure and hardened servers. Security of these servers must be maintained proactively and regularly patched as per international standards and vendors` specifications,
- Authentication and integrity assurance of Domain Name Servers must be of cryptographic origin,
- Hardware Security Module (HSM) shall be used for cryptographic functions, key management and crypto process as per NBSP [V1.0],
- Internet Service Providers, providing recursive name services shall:
    - Employ security hardened servers and maintain their security proactively; and
    - Ensure service provision to authorized and genuine users only.

3.7 Hosting Malware

- Internet Service Providers (ISPs) shall make it sure that no malware is hosted, stored, prepared or available for customers in Pakistan.
- Internet Service Providers (ISPs) shall strictly adhere to the following guidelines:
    - Content having executable scripts, batch files or codes will not be allowed,
    - Content that redirect the internet user to unknown/ malicious servers will not be allowed
- If MoITT came to know about a provider who is hosting malware, MoITT will issue it a written take-down notice (after investigating the matter). After receiving the notice, service provider remove the malware, quarantine the storage system(s) and server(s) or take the system offline within shortest possible time, however this time shall not exceed more than 24 hours.

3.8 Handling Malicious Activity

Internet Service Providers (ISPs) shall ensure that all end-user devices, located and connected to the broadband internet within Pakistan when sustain an attack from malicious node must be quarantined from the broadband internet. Following points must be considered in this regard:

- Pakistan's Broadband Internet Infrastructure, including:
    - Attacks on .PK name servers (ccTLD DNS servers), sponsored or un-sponsored generic name servers (gTLDs DNS servers);
    - Border Gateway Protocol (BGPs) related attacks;
    - Attacks on core components of broadband internet structures, routers or service delivery infrastructure; for example Session border controllers (SBCs) or Voice over IP (VOIP);
    - International Internet Gate Ways.

Chapter - 4

Proposed National Broadband Security Policy [NBSP] v 1.0

This chapter describes **technical control entities** and areas which **MoITT / PTA** needs to enact them on baseline security level. The control areas covered in this policy are following:

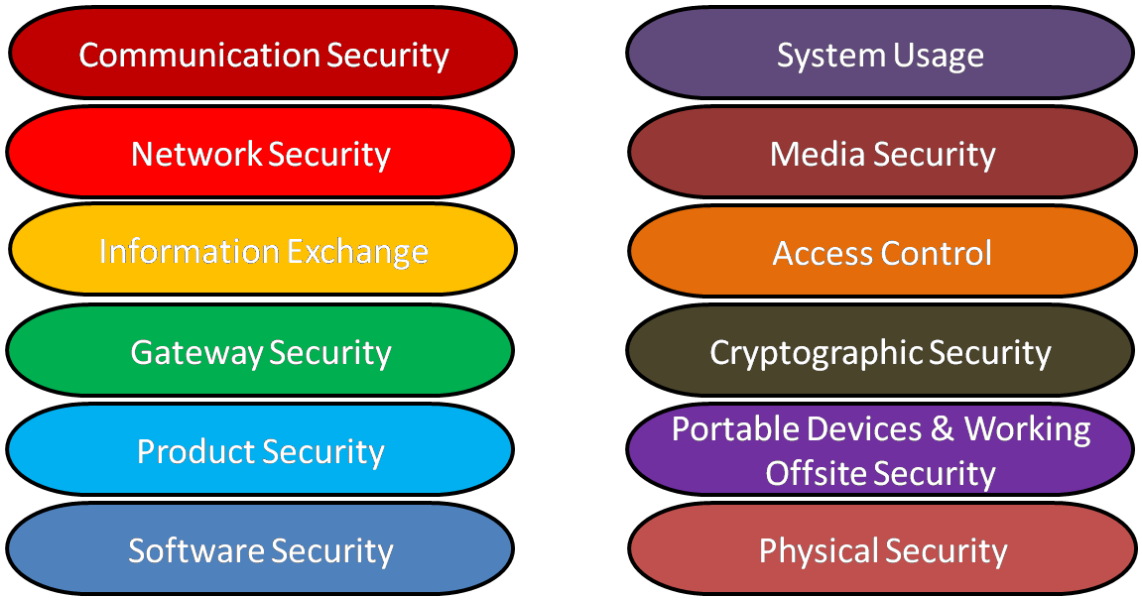

Figure-4.1: Control Areas

4.0 Asset Classification Model

In order to classify the security level and protection of Information Assets, following measures must be taken:-

- Identify the core processes and process owners in the particular organization,
- Identify the process inter-dependencies, for example information, networks, systems, applications,
- Classification of aggregate security level given in table like H, M & L (High, Medium & Low respectively),

- Categorization and full classification of aggregate security level for each asset.

		A0	A1	A2	A3
I0	C0	X	L	M	H
	C1	L	L	M	H
	C2	M	M	M	H
	C3	H	H	H	H
I1	C0	L	L	M	H
	C1	L	L	M	H
	C2	M	M	M	H
	C3	H	H	H	H
I2	C0	M	M	M	H
	C1	M	M	M	H
	C2	M	M	M	H
	C3	H	H	H	H
I3	C0	H	H	H	H
	C1	H	H	H	H
	C2	H	H	H	H
	C3	H	H	H	H

Table 1 – Security Classification Table

4.0.1 Accessibility:

Access to data is described as timely and easy access to data in business hours, for example the up time and availability of data to person(s) who are authorized to access it or for the technical means. Table below describes the key aspects of data availability.

Classification	Availability	Down Time	Response Time
A0	-	-	-
A1	90 %	17 hrs/week	1 to 10 Hours
A2	99 %	2 hrs/week	1 to 10 Minutes
A3	99.9 %	10 min/week	1 to 10 Seconds

Table 2 – Accessibility Classification Table

4.0.2 Integrity:

Integrity of the data means assured correctness, up-to-datedness, authentication and completeness of data. Integrity also guarantees that required data is without unauthorized modifications/ alterations.

Integrity	Class	Action
I0	Source of Information and Time of Changes	Not Important
I1	Source of Information and Time of Changes	Should Be Possible
I2	Source of Information and Time of Changes	Identified and Checked
I3	Authenticity and Integrity	Should Be Provable to Third Party

Table 3 – Integrity Classification Table

4.0.3 Confidentiality

Limitation of information access only to the authorized users and not letting it to unauthorized users to technical entities are covered in Confidentiality domain. The confidentiality of information means access to the data only for authorized persons or technical means.

Confidentiality	Label	Nature
C0	Public	General Public Information
C1	Internal	Material Whose Disclosure Causes Light to Moderate Damage to Affected Party
C2	Limited Access	Access for Defined Users, Material Whose Disclosure Causes Serious Damage to Affected Party
C3	Restricted	Limited Access to a Small Set of People. Material Whose Disclosure Causes Severe Damage to Affected Party
C4+	Top Secret	National Level Security Secrets

Table 4 – Confidentiality Classification Table

4.0.4 Worked Example:

- Let us suppose a particular government entity wants to publish some information of ***Public*** classification; whose particulars of *Availability*, *Confidentiality* and *Integrity* are *A1*, *C0* and *I2* respectively will yield ***Security Classification "Medium"***.
- Government`s data repository which contains Biometric Identities of Citizens will comprise security ratings *Availability*, *Confidentiality* and *Integrity* are *A3*, *C2* and *I3* respectively will yield ***Security Classification "High"***.

4.1 Communication Security

The core objective of this area is to address weakness in physical security and other security issues related with cabling. According to this policy, MoITT/ PTA must ensure that:

CS_1. In order to ensure the physical security, anti tampering, accidental or intentional damage and sabotage; conduits, pipes, and ducts must be used for cable(s) which carry data classified as C4 or above.

CS_2. For systems that deal with data classified at level C4 or above, separate cable(s) and distribution system must be used.

CS_3. Cable conduits installed in public or open places (where access of people is unrestricted) must be labeled in manner that it should not signify the classification of data being carried out it. Also this labeling must not be lucrative/ attractive so it captivates the attention of people who do not possess appropriate security clearance.

CS_4. A detailed register of cable(s) must be properly maintained by the system administrator which contains complete details of floor plan(s), source & destination of cable(s), classification and identification number of cable(s).

CS_5. Inspection of cables be carried out on regular basis with the cable register for addressing any inconsistency.

CS_6. There must be redundant communication media pathways in order to ensure continued connectivity to the broadband internet.

CS_7. Maximum permitted level of classification for conversation on (both internal & external) telephone connections be advised to the user as per level of encryption employed on telephone system.

CS_8. During any telephonic conversation or video call on which information of classification level C3 is conveyed; speaker phone feature must be disabled so the conversation made must not be overheard.

CS_9. It must be ensured that remote initiation must not be enabled for conference systems in sensitive locations.

CS_10. It has to be ensured that rooms where sensitive data is communicated, sensitive documents are placed or meetings are held; must be properly sound proofed so there may be no leakage of sound and no one can eavesdrop.

CS_11. Securing of fax machines using encryption devices on both ends must be used while information of classification level C2 or above is being sent over it.

CS_12. It must be made sure that all standards of document`s classification level, being communicated with fax machine are followed and met at both ends. Further, sender will ensure the following arrangement for the recipient:

- Recipient has to immediately collect the information/ mail from fax terminal as soon as it is received, and
- If fax is not received, recipient will intimate the sender in pre-defined time frame, for example 5 or 10 minutes.

4.2 Network Security

This section of National Broadband Policy V1.0 deals with connections of broadband networks and its general usage. Interconnectivity of multiple networks makes it easy to communicate and provides leverage to the users but this interconnectivity brings in security threat and idea of collective compromise too.

4.2.1 Network Management

To comply with network security domain of NBSP V1.0, MoITT/ PTA must have to ensure that:

NS_1. Details that contain network(s) configurations, layouts, directories (device related or employee related) and all other sensitive technology must not be made available for general public so that unauthorized person may not use these details for any illegal or malicious activity.

NS_2. Default accounts (root, admin etc) are properly disabled and default passwords are changed with new ones.

NS_3. Network manager be sole authority to perform any change in broadband network configuration and all changes are to be made after formal documentation. Record of earlier changes must be kept and maintained for change revision in future.

NS_4. MoITT/ PTA must maintain high level diagram of broadband network connections, a logical broadband network diagram which show all devices and date wise marking of changes made in the network.

NS_5. In order to limit the access and interference of unauthorized persons in broadband network and access to its critical infrastructure, MoITT/ PTA must ensure that:

- Service providers are using network switches instead of hubs,
- All unused ports of switches are disabled,
- Firewalls and routers are segregated and need-to-know rule must be applied over them,
- Use of Internet Protocol Version 6 (IPv6),
- Use of encryption at “Application Level”,
- An automated watchdog tool that keeps check over current implied configuration of broadband network(s) as per:
    - Documented configuration, and
    - Network edged authentication.

- Devices which MoITT/ PTA uses to communicate with broadband network must be connected using “MAC filtering”,
- Service providers` responsibility to look for and countering of any malicious activity within broadband network, and
- Imposing of time and day restriction.

NS_6. Broadband network managers must adhere to the following protection measures:

- Use of dedicated network management devices; for example separate limited area networking (LAN) or using physically separate communication infrastructure, and,
- Usage of secure channels (like Virtual Private Networks VPNs).

4.2.2 Virtual LANs (VLANs)

To comply with virtual LAN policies of NBSP, MoITT/ PTA have to ensure that:

NS_7. To impart separation in Internet Protocol (IP) telephonic traffic and in critical broadband networks, Virtual LANs must be used.

NS_8. Only the most & highly classified Virtual LAN has to be permitted for Administrative Access for the same or lower level classification of network.

NS_9. Risk assessment, implementation of security measures and adhering to hardening procedures recommended by the broadband switch vendor.

NS_10. While using switches, practice of port mirroring or trunking must be avoided during managing Virtual LANs of different level classification.

4.2.3 Multifunction Devices (MFDs)

For an MoITT/ PTA to adhere/ comply with this section of the policy, it has to ensure the following:

NS_11. Multifunction Devices connected to the broadband network must not copy the documents of classification level above of their own classification.

NS_12. Multifunction Devices with enabled ability to transmit information to another broadband network through gateway, MoITT/ PTA must ensure the following:

- Each Multifunction Device is applying its user`s identification, proper audit and authentication of all information sent by user using that particular Multi-Function Device (MFD),
- Above mentioned regulation must be applied over workstations installed at broadband network, and
- The gateway has the ability to identify, filter and then process the transmitted information as per requirements of data export control.

NS_13. Multifunction Devices must not be connected with the telephone line/ device which bear lower classification. However this connection may be permitted after evaluation of MFD using following criteria:

- Implementation of information flow control on MFD so to prevent data flow to unauthorized persons and to unintended destinations.
- Data and information flow control must be capable of segregating the information over its classification and prevent its flow blocking.

NS_14. Multifunction Devices only be deployed after developing/ enacting a comprehensive set of plans, procedures and policies which will govern the usage of these MFDs.

NS_15. C1 level information must not be stored for long periods in Multifunction Devices, configurations and automatic schedules are to be employed for removal of such information from storage of MFD once its job is done.

4.2.4 Domain Name Service Servers (DNS Servers)

To comply with DNS Servers related policies, MoITT/ PTA have to ensure the following:

NS_17. Internal domain information which should not to be disclosed on internet must be kept in a separate internal Domain Name Server.

NS_18. Domain Name Server information which is revealed to the public should bear a secure server which is locally hosted. Government Domain Name Server can be used as primary DNS by state MoITT/ PTA.

NS_19. There should be no single point of failure (logical or physical) in deployed DNS Servers. Security/ hardening of such servers must be proactively carried out and maintained according to international/ vendor specific guidelines.

NS_20. Mutual authentication w.r.t cryptography, digital signing zones of data integrity files must be ensured along with provision of dynamic updates.

NS_21. Authentication of origin of applied cryptography and integrity assurance of Domain Name Server data has to be provided.

NS_22. Only authorized users are to be given access to the zone transfers in DNS service.

NS 23. Cryptographic related functions mentioned in clause NS(20) & NS(21) above, will use a Hardware Security Module (H.S.M) in order to carry out cryptographic process as well as key management.

4.2.5 Internet Security

NS_24. All downloads (files and executables) from the internet must be screened and checked for any potential virus or malicious script. This must be backed by dynamic mechanism for scanning HTTP traffic too.

NS_25. Internet gateway must be capable of denying all unnecessary internet traffic.

NS 26. Internet browsers installed on user end workstations must be updated with latest version and are to be configured properly. MoITT/ PTA must adhere to the following guidelines for configuration of internet browser:

- Java Scripts, auto routing and Active-X activity content must be disabled in browser, unless the source known to be trustworthy.
- Using only up to date browser version and supplemented security patches.
- Discouraging of use of auto-completion and remembering of passwords feature.
- Pop-up blocking, except from trusted sources.

- Removal of cache, temporary and history files regularly in order to maintain data privacy.
- Disabling of auto installation of software and add-ons from online web pages.

NS 27. Browsers must have inherent capability to automatically monitor the ongoing traffic, deduce and pick up traffic patterns and content usage.

4.2.6 E-Mail Security

NS_28. Email servers are to be hardened as per international standards of time and be configured as bastion server(s). Utmost care must be taken in order to avoid disclosure of any system information with external parties through email.

NS_29. Use of TLS protection must be strictly followed with the SMTP Mail server along with Cryptographic Security practice.

NS_30. For implementation of Sender`s Policy Framework, concerned MoITT/ PTA are only to send bounce or undelivered emails for verification through SPF.

NS_31. For reduction in risk of unsolicited emails, intra organization mail distribution list must be kept secure and inaccessible to external entities.

NS_32. Automatic scanning of emails must be carried out by email servers in order to keep them free from any malicious code, script or executable file.

4.2.7 Wireless Security

NS_33. Wireless LANs must be used only with sufficient & necessary authentication and transmission encryptions all together. This process must be complemented with proper security management and adept practices.

NS_34. Wireless security protocols which are considered strong enough to withstand malicious activities such like EAP-TLS and WPA2 are be used with Wireless LANs. But for the integrity of Wireless LAN, reliance on only above mentioned security protocols is not enough. Deployment of automatic mechanisms for dynamic key exchange, and in case of data of classification level C3 or above;

secure Virtual Private Network (VPN) in parallel with wireless network recommended.

NS_35. Inventory of all devices having "Wireless Interface Cards" (Wifi Modems) must be maintained properly and if any device goes missing, change in encryption keys must be done ASAP.

NS_36. Network Administrator must regularly scan and monitor the access points for any unauthorized or rogue WAP.

NS_37. Location of access points be made so that their location can-not be traced from publically accessible areas to avoid "network tapping".

NS_38. Settings & configurations of client end for 802.1xx standard protocols are to be kept secured through all aspects. This can be done by disabling the installation of new security certificates.

NS_39. SSID of any network should not reveal the organization it belongs to. And on the very initiation of wireless access point connection, following defaults must be changed:

- Default Name,
- Simple Network Management Protocol, and
- Community Strings.

NS_40. In case of non public wireless access point, SSID broadcast should be disabled and encryption keys must be changed on regular intervals. Media Access Control (MAC) filtering can also supplement this scenario.

NS_41. For playing a mediatory role, filtering of traffic and security purpose, a router must be placed between the MoITT/ PTA`s network and particular access point and only required ports are to be enabled via restricted firewall protocols implementation.

NS_42. Installation of WIPS and/ or WIDS aids are highly favored for those networks which deal with information of classification level C3 and/ or higher level in

order to monitor threats like rouge Applications and DOS attacks, being posed against wireless installations.

NS_43. Multiple SSIDs from a single network with different configurations for different Virtual LANs is strongly advised. Different authentication methods are to be implied too, for example a guest user may be granted lower security and limited access to internet.

4.2.8 Clock Synchronization

NS_44. Best practices (as per international standards and/ or vendor specific) for securing of NTP servers must be followed.

NS_45. If a computer or communication devices carries real-time clock, it must be synchronized to Universal Time Coordinated (UTC) or local time standard. Some clocks have inherent drift which must be accounted for any variation.

NS_46. Pakistan Standard Time (PST) can be used as primary clock reference for NTP Server.

4.2.9 Virtual Private Networks (VPNs)

NS 48. Any Virtual Private Network (VPN) which is set to deal with information of C3 or above level must implement 2-factor verification in following manner:

- **Factor-1:** One-Time-Password Authentications (like pass-phrase, public-private keys or device token systems).
- **Factor-2:** Username and password with the help of external authentication server like TACACS, Radius etc.

NS_49. Virtual Private Networks (VPNs) must be configured to auto-disconnect after a pre-designated time interval of inactivity and for access, user has to login again.

NS_50. MoITT/ PTA must allow one network connection at one time. Split connections and tunneling must not be allowed.

NS_51. All workstations in connection with MoITT/ PTA`s core network through Virtual Private Network has to be equipped with Anti-Virus and security

software whose patches are updated and their virus definitions and signatures are up to date.

NS_52. To control network traffic from information server or system to Virtual Private Network (VPN) client, firewalls at gateway level be installed.

4.2.10 Voice over IP Security (VoIP)

NS_53. Voice channels and data streams are exclusively separate networks. These two streams of networks must be kept separate physically; however use of Virtual Private Network (VPN) between them is permitted. Voice gateway domain interfaced with Public Switching Telephone Network separates protocols of SIP, H.323 and other similar class voice protocols from data network stream.

NS_54. Security measures and mechanisms in Voice over Internet Protocol capable gateways must be employed.

NS_55. Unnecessary voice protocols must be disabled and use of Secure Real Time Protocols (SRTP) be carried out to evaluate the security and integrity of system.

NS_56. In order to protect the VoIP infrastructure, proper physical countermeasures are to be employed.

NS_57. Proper log of calls made over VoIP be maintained.

NS_58. If permitted, soft phones only to be used with secure Virtual Private Network (VPN).

NS_59. In case of power failure, adequate power backup must be readily available for VoIP phone devices.

NS_60. Voice gateway systems must be secured with strong authentication and proper access control.

NS_61. Secure Shell Host (SSH) or IPSEC must be used for all management and auditing of system remotely.

NS_62. Backup contingency plan must be kept on standby for voice calls in case of VoIP failure.

NS_63. Network LAN switches must be enabled with port security features for VoIP devices.

4.2.11 Internet Protocol Version 6

NS_64. Complete risk assessment must be carried out by MoITT/ PTA to determine the security wise merits and de-merits of both TCP/IPv-4 & TCP/IPv-6 network technologies. IPv6 technology must be considered by MoITT/ PTA for deployment.

NS_65. For implementation of a dual stack environment, complete risk assessment must be conducted.

NS_66. Upon implementation of IPv6, recertification will be considered by MoITT/ PTA.

4.3 Information Exchange

This section of NBSP V1.0 defines laws and baseline security rules that how sharing of critical information will be done with government MoITT/ PTA and other stake holders/ third parties.

4.3.1 Policy & Baseline Controls

IE_1. MoITT/ PTA will evaluate and understand the infrastructure, domain, risk and security of domain prior to establishing connection with it. Reviews and observations made during this evaluation step must be logged and documented for future reference and review.

IE_2. Before initiating a cross-domain connection, MoITT/ PTA will take into account all the networks which are associated/ connected with the domain the MoITT/ PTA is going to connect. Special care must be taken when a trace of un-intended and cascaded connection is observed. Most particularly where traces of connection with un-trusted network(s) are obtained.

IE_3. MoITT/ PTA will make it sure prior to connection establishment for data exchange that all necessary agreements (including confidentiality agreement) and documentation between the entities have been finalized. The documentation

and agreements must explicitly chalk out procedures of information exchange, liabilities & responsibilities of parties involved, technical standards, matters of ownership and ultimate control. In case 3rd party entity or outside vendors are involved; an agreement of Non-Disclosure of Information & exchange will be formally implemented.

IE_4. It must be made sure prior to initiation of information sharing that media used must be fool proof and immune to unauthorized access or misuse.

IE_5. Strict measures to be taken for protection and classification of information which has been obtained from other MoITT/ PTA.

IE_6. MoITT/ PTA must make it sure to arrange appropriate measures for physical security of information passage media and storage. Information must be stored in fashion that packing maintain its integrity at all and keep it away from any hazard which may render this information unreadable/ useless.

IE_7. Only authorized courier service(s) be employed for the passage of information and proper list of trusted courier services be maintained.

IE_8. Protection of information from unauthorized access, alteration or interruption; when it is being exchanged through electronic media.

IE_9. While transmission of information of C-3 or higher level, MoITT/ PTA must ensure implementation of secure messaging (in which information is encrypted and/or digitally signed). For this purpose, MoITT/ PTA are advised to implement “Secure Multipurpose Internet Mail Extension (S-MIME)” or any other robust security protocol of time.

IE_10. In all out bound mails, a disclaimer note (template given below) must be appended:

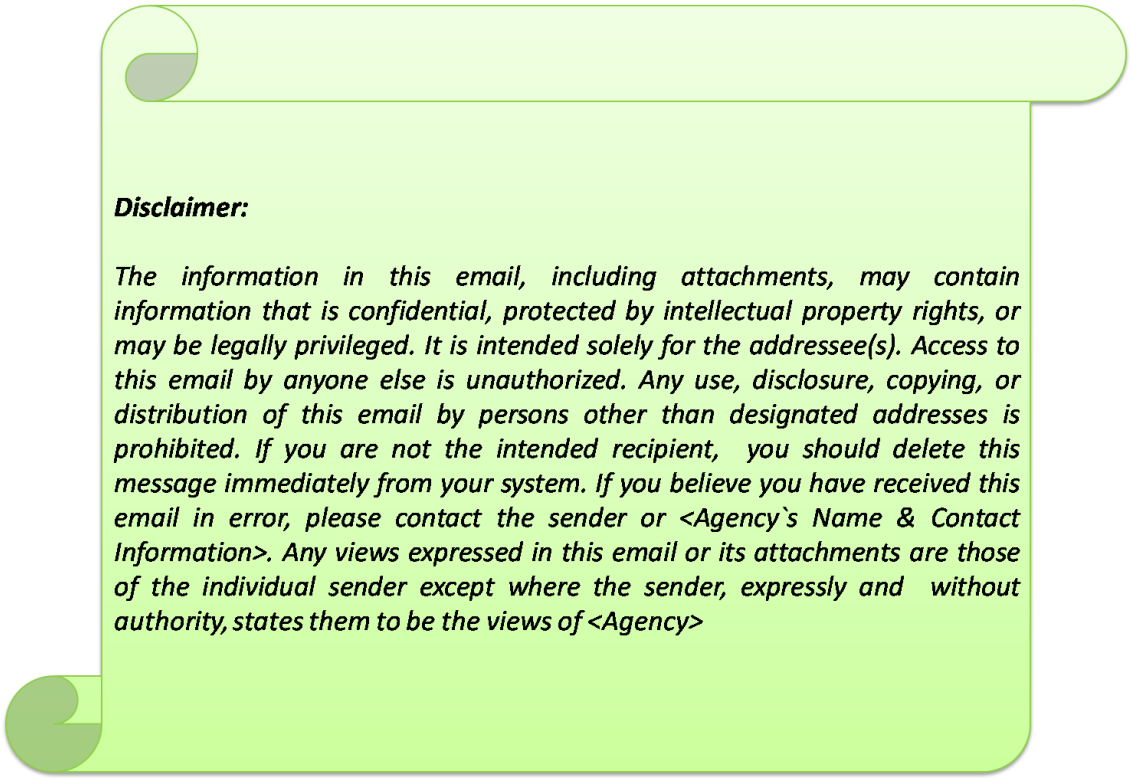

Figure-4.2: Disclaimer Template

IE_11. Information dissemination must be carried out with utmost diligence in order to ensure sanitization of information (irrespective being sent or received)and removal of of viruses, .bat or other scripts, and Trojans etc codes.

IE_12. It must be ensured by the MoITT/ PTA that information is immune to any attempt of unauthorized access during its transfer. If the data being transferred is of Confidentiality and Integrity level 2 & 2 respectively; end-to-end encrypted channel must be utilized as already discussed in Cryptographic Security part of this policy.

IE_13. Only a designated and trained media representative has to provide the information, after its sanitization to the public and media outlets.

4.4 Gateway Security [GS]

This portion of NBSP V1.0 provides minimum thresholds of security requirements in order to secure the gateways which are used to transfer the data among

MoITT/ PTA as well as communication with external world. This enables the flow of allowable information and subsequently preserving the need-to-know requirement. Gateway equipment includes Proxies, Content Filtering Algorithms, Routers and Firewalls.

4.4.1 General Conditions

GS_1. Protection of network from outside world networks by using gateways along with strict control on data stream flows.

GS_2. For the gateways that are used to create connection among MoITT/ PTA` servers or with the un-controlled network, following conditions must be enabled:

- Usage of appropriate device for controlling data flow.
- Proper control over data flow.
- Placement of gateway hardware in physically secure server rooms.

GS_3. Maintenance of gateways must only be carried out by authorized / trained staff.

GS_4. Dual control and four eye principle be applied while providing management and/ or administrative access to the gateways which deal with information of C3 or above level.

GS_5. Labeling of information exchanged from gateways shall be done according ot the National Information Classification Policy and protected. Classification of gateways must be in-lined with the information transmitted through them.

GS_6. For making separation between systems which can be accessed externally and unwatched public network and internal networks; use firewalls and likewise security equipment. This separation setup is termed as Demilitarized zone (DMZ).

GS_7. Gateways:

- Must be the only path between internal and external world.
- Have ability to deny any connection attempt from either inside or outside.
- Allow only authorized connections to establish.

- Must be managed via a secure and separate path from the rest of network.
- Be able to detect security breaches and any foreign network intrusion.
- Provide event triggered real-time alarms.

GS_8. Gateways must be hardened and protected against:

- Threat of malicious scripts and software vulnerabilities.
- Improper or poor configuration of hardware.
- Privilege Escalation and Compromise/ breach of account.
- Monitoring of rogue network(s).
- Attacks of "Denial of Service (DoS)".
- Leakage of information and/or data.

GS_9. Ensure proper monitoring, supervision and management of gateways. Also there must be log records, danger prevention mechanisms, alerts and watch over on associated equipments.

GS_10. Gateways must have capability to automatically block or trash any data which is categorized as "suspicious" including:

- Offensive content, attachments or language used.
- Content infected with malware or ransom-ware.
- Denial of Services (DoS) attacks.
- Content belonging to categories which are declared inappropriate by laws and authorities of Pakistan.

4.4.2 Data Export

GS_11. System/ Application users:

- Are liable and will be held accountable any data they export.
- Are strictly instructed to carry out protective markings/ seals check, carry out visual inspections and checks of metadata to assure the relevancy of data being exported.

GS_12. Data exports are either performed under:

- Laws and regulations imposed by government MoITT/ PTA; or
- Laws approved by information security manager.

GS_13. On basis of classification, export of data is restricted when it is being transferred to less classified system.

GS_14. Data export must be checked for ensuring that:

- Search is carried out by entering entirely textual data.
- Quarantine of data which is unidentified till is reviewed by a trusted source or originator and released only then.

4.4.3 Data Import

GS_15. All system users who import data are:

- Are liable and will be held accountable any data they import.
- Are strictly instructed to carry out protective markings/ seals check, carry out visual inspections and checks of metadata to assure the relevancy of data being imported.

GS_16. Consider the following during data imports:

- In strict accordance with procedures and practices approved by the MoITT/ PTA; or
- Laws & regulations devised by information security manager.

GS_17. Always carry out scan of the data for any active content or malicious scripts; which is bound to be imported to MoITT/ PTA`s system

4.5 Product Security [PS]

This part of policy set minimum security standards for selecting and acquisition of information products and related hardware. MoITT/ PTA are to ensure that products selected through the process meet the security standards set by the policy and fulfill the independent evaluation criteria listed as per NBSP V1.0.

4.5.1 Policy & Baseline Controls

MoITT/ PTA are to ensure the following:

PR_1. Due diligence must be observed while selecting the product and ensuring independence of vendor.

PR_2. Classification and labeling of products have been done as per standards set by National Information Classification Standards.

PR_3. Identification, screening and evaluation criteria of vendor(s) should include:

- Ownership and location,
- Financial situations,
- Reference and comments from pervious contracts/ engagements,
- Ability to devise and maintain proper control, determined after analysis of risk assessment.

PR_4. In order to avoid any loss to confidentiality or integrity, enhanced testing and operational equity between device functionality and verification of any claim made by vendor must be done.

PR_5. Security evaluation of under consideration device be carried out on security tests, functionality and performance tests, checks on vulnerabilities and immunity against potential threats.

PR_6. Delivery of the product must be made in accordance with MoITT/ PTA`s practice for secure delivery process.

PR_7. Delivery process must contain measures to identify tampering attempt(s).

PR_8. Products are purchased from only those developers/ vendors who have commitment to provide assured future maintenance of their products.

PR_9. Product patching and security updates are to be readily available.

4.6 Software Security [SS]

Chief concern of this portion revolves around security during process of software development and acquisition. These policies define and supplement different phases of system and life cycle development of software (SDLC). Also this section covers the security control for other commercial application of products outside scope of MoITT/ PTA application(s).

4.6.1 Software Development & Acquisition

Concerned MoITT/ PTA must ensure that:

SS_1. Security must be of prime concern during all phases of SDLC.

SS_2. No matter new, old or under-development; all applications have to be given classification using the standards defined in **"Asset Classification Model"** w.r.t **Integrity, Confidentiality** and **Availability**.

SS_3. Security requirements must be developed & implemented; including functional and technical aspects as an integral entity of system requirement.

SS_4. Testing, evaluation and development infrastructures of the software and its related data must be carried out over dedicated infrastructure fully separated from production line. Passage of information between these two system domains must be restricted and limited to predefined policy. Access to the administrative/ management source shall be disabled.

SS_5. Any software application only to be made available for production after is clears security and quality assurance tests and checks which will confirm the working of application according to the security standards.

SS_6. Software developers must adhere to secure coding practices and must consider the following points:

- Fully adopt the best practices and consult the forums where professional programming practices and their errors are discussed,
- Design the software in such way that is use lowest level privilege needed to perform its assigned task,
- Denial of access to system by using default credentials,
- Verification of return values of all calls provided by software, and
- Clarification of exceptions and validation of all inputs.

SS_7. Before being used in production, software should be tested in all aspects for its functioning and vulnerabilities. For enhanced evaluation, an independent party may carry out the requisite testing (not by the developer!)

SS_8. All Software (purchased and/ or developed) must comply with all legal requirements and pre-requisites.

SS_9. All systems (purchased, obtained and/ or self-developed) must be documented sufficiently for any handy reference.

SS_10. Source code (not the binary or any other combined file(s)) of custom developed applications must be available all the time and MoITT/ PTA may review this code in case of any issue raised.

4.6.2 Software Applications

In area of software application, MoITT/ PTA are directed to ensure:

SS_12. All servers, workstations, their security objectives, working mechanisms and other necessary logs must be documented properly and be placed in system security plan.

SS_13. Workstations must be placed inside a hardened standalone "Standard Operating Environment (SOE)" which can:

- Carry out removal of unwanted software,
- Disable unused and/ or undesired functions of system software and application software,
- Implying access control over system objects which effectively reduce system user and programs to perform their tasks/ functionalities with minimum access,
- Limiting of inbound and outbound network connections by using software based firewalls,
- Configuration of local event log or remote logging to the central server.

SS_14. Potential vulnerabilities in systems and their "Standard Operating Environment (SOE)" can be reduced by:

- Restrictions on unnecessary file shares.
- Timely patching of software.
- Barring access rights and controls to all needless in/out functionalities.

- Removal of unused and/ or dormant accounts.
- Renaming of accounts with default username(s).
- Changing of default passwords.

SS_15. High risk servers which are dealing with Web browsing, email handling, file transfer, Internet Protocols, Voice-over-IP telephone servers and connectivity to unwatched public networks must ensure that:

- Maintaining proper separation on basis of functionality among servers so they work independently and if one among them gets infected, other may keep working.
- Limit the communication among servers both at file system level and network and minimum access must be given to the user which is enough for user to perform job.

SS_16. Carry out classification and checking the server`s integrity which are vitally important to the MoITT/ PTA and are on verge of compromise or sabatoge.

SS_17. Integrity information must be stored in a secure manner off the server.

SS_18. As soon as legitimate change(s) are made to in the system(s), updating of integrity information be updated.

SS_19. During MoITT/ PTA's audit, comparison of earlier stored integrity information and current situation must be done on order to validate the functionality and rule out any compromise to the system.

SS_20. Upon detection of any change, all necessary steps in its mitigation must be carried out in accordance with information and communications technology of concerned MoITT/ PTA and other security procedures.

SS_21. All software application are thoroughly checked to ensure they are do not try to establish any connection to the outside world or not, and if it does so; MoITT/ PTA must make decision to either permit or deny this connection attempt by considering all the involved risks generated by this connection (if any).

4.6.3 Web Applications

Regarding Web Based Applications, MoITT/ PTA are to ensure that:

SS_22. Each and every content placed on their web server is thoroughly evaluated for all security related issues. For building a secure web services and applications, MoITT/ PTA can take guidance from Open Web Application Security Project (OWASP).

SS_23. Interconnectivity and access between web application and their components must be minimized.

SS_24. During transmission, make it sure that sensitive data and personal information is stored using standard cryptographic controls.

SS_25. Authentication of critical sector websites must be strongly authenticated. For this authentication, SSL certificates can be obtained from service providers licensed in Pakistan.

SS_26. Any application which bears medium or higher risk rating(s), must be used with Web Application Firewall (WAF).

4.6.4 Databases

For ensured security and working of database, MoITT/ PTA should:

SS_27. All information which is stored in database must be related with proper classification of category if the particular information:

- Can be transferred to other system(s), or
- Bears multiple classifications and/ or multiple handling requirements.

SS_28. MoITT/ PTA must make it sure that appropriate level and handling requirement of any information whether it is exported or retrieved from database must be dealt in accordance with its classification level.

SS_29. Database bearing files should be kept well from any access type that has ability to bypass the access control of database; by applying all security means.

SS_30. There must be functionality in database thorough which it can execute audit of actions performed by user actions.

SS_31. If database fails to respond to a query or applied filter properly, sanitization of query results must be ensured by the MoITT/ PTA for meeting the minimum allowed security privilege to that particular user.

SS_32. The information in database which has classification level C3 or above shall be masked by employing state of the art masking technology available at that time.

4.7 System Usage Security [SU]

This section of the policy deals with the definitions of behavior and attitudes which are allowed during system usage. It is the responsibility of the concerned MoITT/ PTA to ensure that users are well aware, properly trained, and understand the obligations pertained upon them.

4.7.1 Policy & Baseline Controls

For system usage security and control, MoITT/ PTA must ensure the following things:

SU_1. System and/ or workstation user shall be full responsible for the information assets (both system(s) and its related infrastructure) provided them to perform their official tasks. They are bound to use said information equipment with due care and within perimeter set by vendor(s) and/ or MoITT/ PTA`s usage policy.

SU_2. While surfing the web browser, user shall strictly follow and comply with the internet surfing policy guidelines issued by the MoITT/ PTA. It is upon the discretion which sites are to be accessed (like SMN sites, news feeds etc).

SU_3. Information and Computer Technology assets must be protected against web based threats (malwares, Trojans and worms) by barring the download of software, executables and scripts.

SU_4. Access to the web must only be made using filtering gateways and secure proxies.

SU_5. MoITT/ PTA`s staff must be fully abreast of permission regarding web content types which they are liable to access. For monitoring the content accessed from encrypted channels, MoITT/ PTA should consider a viable and effective solution.

SU_6. Usage of email must be done with utmost and due diligence and their content be treated as their classification label set by National Information Classification Policy.

SU_7. Proper check must be carried out before opening any email for potential/ possible threat(s). If there surfaces a threat (for email carrying Trojan, spam, virus, scripts, root kits, malware or social engineering content) in email, appropriate measures must be taken.

SU_8. Staff must ensure and adhere to the policy that public e-mails must not be generated or received from MoITT/ PTA`s systems.

SU_9. Staff will make it sure to that ant email which contains critical information should only be sent to the designated user on his/ her name and must not be sent in group mail.

SU_10. Staff will make it sure that email who carry information of classification level C2 or above must not be forwarded automatically outside MoITT/ PTA`s domain.

4.8 Media Security

Objective of media security framework is to aid MoITT/ PTA in defining how the media is classified, tagged/ labeled and documented/ registered for proper identification. Not only just classification but even this policy takes into account complete lifecycle of media content and its usage, repair/ modification, sanitization, archiving and final destruction.

4.8.1 Policy & Baseline Controls of Media Classification and Labeling

MS_1. Any hardware that contain media will be classified as per the media content`s classification it contains.

MS_2. Non-volatile media hardware will be labeled with highest security classification w.r.t the information stored in that non-volatile media.

MS_3. In Volatile media`s scenario, till it is powered by source it will be having highest classification while its power is on. Once its power is removed, same volatile media will be treated at C1 classification.

MS_4. Re-classification of storage media can be done if:

- Information copied to that media bears a higher classification, and
- Information stored in that media is subject to classification level up gradation.

MS_5. Media hardware devices which bear classified information de-classified if:

- On consent of the media owner to de-classify it, or
- The media has been sanitized

MS_6. If information on storage media can-not be sanitized (due to media hardware nature), it must be destroyed as the information over it can-not be de-classified.

MS_7. Classification of media must be done in a way that it should be readily visible and identifiable. MoITT/ PTA may use protective marking in this regard.

MS_8. While using non-textual representations for media classification and marking(s) amid operational security, MoITT/ PTA are required to train their staff members accordingly in labeling scheme(s).

4.8.2 Media Sanitization

For sanitization of media and its related hardware, MoITT/ PTA must:

MS_9. Properly document the procedures that MoITT/ PTA follow for sanitization of media and this must be regularly tested.

MS_10. All media hardware device types, containing information of classification of C1 or higher should be fully perished/ shredded prior to their disposal. These media include(s):

- Microfilm &Microfiche.
- Optical discs (Both CD & DVD).
- Printer ribbons.

- Carbon Papers.
- Impact surfaces which face the platen.
- Programmable Read-Only memory (PROM) & Read-Only memory (ROM) devices.
- Flawed/ defective media hardware which can-not be sanitized.

MS_11. Sanitization of volatile media can be achieved by:

- Disconnecting power from media device for long periods (at least 10 minutes) , or
- Re-writing of media with random patterns and re-verification of overwriting by reading the data contents.

MS_12. For magnetic non-volatile media sanitization:

- Simply just overwriting the media, if pre-2001 or under 15GB storage capacity, re-writing of media with random patterns for almost three times and re-verification of overwriting by reading the data contents.
- For overwriting the media hardware manufactured after 2001 or having storage capacity of 15GB, re-writing of media with random patterns for just single time and re-verification of overwriting by reading the data contents.; or
- By using electronic / electrical de-gaussing equipment with strong magnetic field strengths for total disruption of the magnetic media.

MS_13. For sanitizing non-volatile Electronic Programmable Read Only Memory (EPROM), application of ultraviolet rays more than vendor/manufacturer specific times in factor of three and then infesting media with random patterns. Sanitization of EPROM media which had C3 or above information must be documented properly.

MS_14. Flash memory sanitization can be done by over-writing the media with pseudo random pattern, formatting it, then again writing a pseudo random pattern. Open source software (for example Viper) can be used for this purpose too.

4.8.3 Media Repairing and Maintenance

Following are the policies which must be abide by MoITT/ PTA in order to carry out repair and maintenance of Media hardware:

MS_15. Only a vetted, well trained and briefed person(s) should carry out repair and maintenance of media hardware which contain classified information

MS_16. Repair of any system which contains information of C3 or above must be carried out under supervision.

4.8.4 Media Destruction & Disposal

To ensure proper destruction and disposal of obsolete/ unwanted media hardware, MoITT/ PTA must:

MS_17. Properly document the procedures and steps followed for the destruction a7 disposal of media.

MS_18. For destruction of media hardware:

- Magnetic Deguassing of non-volatile media,
- Physically damaging/ shredding the media, and
- Heating/ burning the media so its internal components melt or turn to ashes.

MS_19. Members of the committee which is overseeing the destruction process of media:

- Carry the media hardware personally to the destruction point.
- Ensure successful & total destruction of media hardware, and
- Must document the destruction of media which contained information of level C3 and above.

MS_20. Media hardware must be sanitized up to possible level before its destruction.

MS_21. Destruction and disposal process of media be carried out in a way that it should not attract the unwanted attention of irrelevant people.

4.9 Access Control Security

This control set of policy is to use the deployment and implementation of several solutions to control access for maintaining the integrity, availability and confidentiality of MoITT/ PTA`s top secret/ secret & prime information assets. Further there are rules which are necessary to attain this protection for a secure, smooth, reliable and robust operation of MoITT/ PTA`s Information System(s),

4.9.1 General

To comply with the access control security protocols and rules, MoITT/ PTA must:

AM_1. Provide access to the user based on concept of "least privilege", and further govern it over "Need to Have" or "Need to Know" basis.

AM_2. Access to the system has to be controlled and managed using system`s access control, identification, authentication, and comprehensive audit runs w.r.t information`s sensitivity which is stored into that system. Request for system access shall be processed by manager or at least supervisor level staff member.

AM_3. Hierarchy based model must be implemented in order to spread access rights for data creation, alteration, updating, deleting or transmission of MoITT/ PTA`s information.

AM_4. A comprehensive setup must be established which describes role of employee to the information access and change of his/ her role. For example what will be access level of an employee when he/ she is promoted, demoted or terminated.

AM_5. In order to attain special access bypass from security mechanism no matter what the reason(s) it may be, formal authorization from security manager of MoITT/ PTA must be taken.

AM_6. Unauthorized access attempt to the MoITT/ PTA`s control in an illegal manner shall be treated as security mishap and shall be handled strictly according to the organization`s policy in this regard.

AM_7. Maintenance of audit logs will be carried out in a manner so that is shall allow a convenient assist in its monitoring as per rules devised by the government MoITT/ PTA and devised practices of incident management.

AM_8. While accessing MoITT/ PTA`s Network through logical access (which is technically controlled), Network Admission Control (NAC) services and devices can be used.

AM_9. Secured records must be maintained of the following:

- Of all authorized system users and their identification,
- The person who sanctioned access to these users,
- When the said authorization was given?, and
- To which system the access was granted?

AM_10. There must appear a banner before logon or access to the system is granted. This banner must contain that:

- Access to this system is permitted to authorized users only,
- Agreement containing security policy which a system user has to abide,
- Notification regarding monitoring of user activity,
- Legal ramifications and punishments of violating the policies of system user agreement, and
- An acknowledgement from user.

AM_11. Critical entities of the information infrastructure like centralized authentication repositories (like LDAP) and authentication database(s) should be protected from attacks of "Denial of Services (DoS)" and must employ authenticated and secure channels for data retrieval. An automatic log must be maintained in such repositories record the following events:

- Unauthorized and/ or illegal access,
- Start and end time of such activity,
- User identification in case of illegal logon attempt,
- Login & logout activities in case of illegal logon attempt, and
- Initiation and termination of remote session(s).

4.9.2 Identification & Authentication

AM_12. A set of policies which maintain policies and plans to cover the system users` identification, authentication, and authorization in order to keep track of user`s credentials.

AM_13. MoITT/ PTA must educate their system users regarding procedures and policies enacted by the MoITT/ PTA they work for.

AM_14. It must be kept in mind that all the users bear unique identity and are authenticated on each session in which the user is granted access to a system.

AM_15. Unless approved by the security manager of the MoITT/ PTA, access to the information repository must not be granted to the persons who do not belong to the MoITT/ PTA on regular grounds (like contractors, daily wagers and consultants etc). Security Manager will too check the required and essential information, documentation and agreements giving access to them.

AM_16. Areas where no specific or shared accounts are used, there alternate methods be applied for identification of the user(s).

AM_17. Authentication information, which can be used/ grants system access or decryption of an encrypted system and is unprotected must be taken into special care.

AM_18. Any information/ system which is not in use is always susceptible to cyber & malicious attacks and session-hijack.

AM_19. Recommended strength of a password is 12 characters at least without adding-in any complexity. However in case of complex password pattern, at least 7 characters along with following can be used:

- Upper & Lower Case letters (Aa, Zz),
- Digits (from 0 to 9),
- Punctuation marks and special characters.

AM_20. Minimum duration for password change is ninety (90) days.

AM_21. Password changing request will be entertained only single time in 24 hours and system will prompt the user to change the password both on the very first login as well as on verge of expiry.

AM_22. While choosing passwords, following points must be considered:

- Avoid using predictable hints for password reset,
- Reusing of same password for resetting of multiple accounts,
- Re-iteration of old password, and
- Using of sequential passwords.

AM_23. Manage screen locks and session logs so that:

- It gets activated after specified time (like 5 minutes) of inactivity,
- Can be activated manually,
- Lock must be able to conceal all the statements and access controls,
- Screen must remain lit while locked,
- System user re-authentication while unlocking, and
- Denial of the user ability to disable/ override screen/ session locking mechanism.

AM_24. There must be limited tries for user to login and after these are out, access to the system must be suspended.

AM_25. In case the password is lost or compromised:

- Immediately inform the system administrator or the concerned individual for suspension/ freezing of account, and
- Password reset must be done after re-verification of user identity.

AM_26. Any account which remains inactive/ dormant for more than 90 days must be suspended.

AM_27. Audit of the account(s) which process or deal with information of level A2, I2 or C2 must be carried out on bi-annual basis.

4.9.3 System Access

This section defines the rules which govern system access and concerned MoITT/ PTA must take into account that:

AM_28. For access to any security policy, briefing or its related documentation, security clearance of user must be necessary

AM_29. Personal security of the system user must be vetted before granting of access to system.

AM_30. System users must be given brief on system before access being granted to them.

4.9.4 Privileged Access

In order to confer "Privileged Access" to the user(s), MoITT/ PTA must com must ensure:

AM_31. Properly documented, controlled, accountable and minimum access to the privileged account(s).These accounts must be used for carrying out administrative or management nature jobs only.

AM_32. System administrator must be assigned with a designated individual`s specific account for performing/ undertaking their specified administration task(s).

AM_33. Privileged access to the system(s) which process or carry information of level C4 or above must be given exclusively to Pakistani nationals only.

AM_34. A proper system management log must be maintained and made to record the following:

- Sanitization/ purge activities,
- System`s boot and shutdown,
- Failure of system or its component(s),
- Activities regarding system maintenance,
- Process of backup creation and archival of key data activities,
- Activities related to system(s)/ file recovering, and
- Odd/ unusual hours activity.

4.9.5 Remote Access

While managing remote access to the system, MoITT/ PTA must consider that:

AM_35. Remote access should not be granted except sheer business requirement or explicitly authorization by MoITT/ PTA head and with due diligence.

AM_36. For remote access, two factor verification must be applied which must be supplemented by biometric control, hardware token(s) or any word-aid when remote access is being granted to the system which has information of level C3 or above.

AM_37. Remote access session(s) must be secured with sophisticated end to end encryption of ongoing standard.

AM_38. Remote access systems are to be equipped with sophisticated Anti-Virus and must maintain a personal firewall. These two security features must remain active all the time and set to work in automatic mode.

AM_39. All security software installed on systems with remote access enabled must be patched/ updated on regular basis.

AM_40. Users of remote access systems must not access to the MoITT/ PTA`s internal system(s) or copy its contents to any other public system/ computer.

AM_41. Vendor of the system must be granted remote access only when there is no other choice/ alternate way. This access must be clearly defined (duration and nature of task) and must be monitored and controlled by the concerned MoITT/ PTA.

4.10 Cryptographic Security

4.10.1. Policy Objective

Processing of information in digital world is not secure unless encryption is used. This section of NBSP V1.0 describes baseline for implementation of encryption techniques in order to keep vital information confidential, secure and integral in the cyber world which is infested with vulnerabilities and threats.

4.10.2 Policy & Baseline Controls

CY_1. Encryption of hardware and software, use of cryptographic algorithms, digital signatures and key management procedures must meet the requirements of MoITT/ PTA and are to be according to international standards of the time.

CY_2. Specific time duration must be set for key revoking and in case of suspected compromise to the system; keys must be replaced as soon as possible.

CY_3. C3 or above classification information assets are to be encrypted and fully protected while stored/ in transportation against unauthorized breach or illegal access to them, no matter which storage media or format are used. MoITT/ PTA can further apply cryptographic controls to its information assets if it seems necessary after risk assessment.

CY_4. I3 or above classification information assets must be secured by the use of cryptographic hashing(s). MoITT/ PTA can further apply cryptographic controls to its information assets if it seems necessary after risk assessment.

CY_5. Following protocols must be considered while transiting of C3 or above classification information assets:

Situation	Protocol
Security of web traffic	T.L.S (128 or 128+ bits); [RFC4346]
Security of file transfer	S.F.T.P
Securing remote access	S.S.H-v2; [RFC4253] I.P.S.E.C; [RFC 4301]
Securing emails.	S/MIME-v3; [RFC3851] or latest version

CY_6. Security of passwords by using hashing & encryptions during their stored/ in transportation against unauthorized breach or illegal access to them, no matter which storage media or format are used. Privileged passwords (if any) are to be stored off-site and encrypted and backed-up for ensured recovery.

CY_7. Applications where usage of Hardware Security Modules (HSMs) is carried out, these modules should be certified to minimum standards of FIPS_140-2 Lvl-II or Common Criteria [CC3.1] _EAL4 security standard.

CY_8. Keys of Cryptographic algorithms are only to be transited physically and in strict accordance with CY_5

CY_9. Proper key management system must be used to effectively manage the cryptographic key`s life cycle. Following points must be considered:

- Definition of roles and duties of key custodian,
- Process of key generation,
- Splitting knowledge and usage of dual control,
- Secure storage of key,
- Proper key usage,
- Transition, distribution, recovery and backup of secure keys,
- Periodic inspection of key status,
- Revoking and obliteration of key(s), and
- Documenting and audit trail of keys.

CY_10. MoITT/ PTA will make it sure to check the certification and compliance of digital certificates as per international standards. Online revocation system must be used in order to minimize the illegal use of digital certificate(s).

CY_11. Any smart card or security token which provisions the systems of CSP must meet the requirement of Subject Device Provision Services standards, defined in [CWA14167-1].

CY_12. While using digital certificate in any production system; it should have a CSP license issued in Pakistan.

4.11 Portable Devices & Working Off-Site Security

4.11.1 Policy Objective

This section deals with the requirements and standards for mobile/ portable equipment (like laptops/ palmtops and cell phones etc) while these are being used within MoITT/ PTA`s premises and other controlled/ uncontrolled environment(s).

4.11.2. General Rules

MoITT/ PTA are liable to ensure following conditions while governing portable devices:

OS_1. Policies must be defined for how the mobile devices and other likewise devices will be used in MoITT/ PTA.

OS_2. Classified conversation must not be conducted over the mobile devices which have capability to conduct phone calls.

OS_3. All the laptops and mobile devices which possess critical information, their Bluetooth and serial connection port must be disabled.

OS_4. All the laptops and mobile devices which bear recording ability must not be allowed or brought in areas of high risk and if it becomes necessary, it should be brought after approval from MoITT/ PTA`s Security Manager.

OS_5. Laptops and likewise mobile devices have to encrypt the stored information password enabled login must be implemented.

OS_6. Mobile and likewise devices are to be kept under permanent & personal supervision of MoITT/ PTA`s Security Manager when being used or kept secured while not in use.

OS_7. All the laptops and mobile devices, which the MoITT/ PTA do not own are not be connected with the MoITT/ PTA`s own computers/ networking systems at all. However, temporary connection can be made only in necessary situations and the connection must be protected by firewall to prevent any threat.

OS_8. Un-accredited laptops and mobile devices must be used to save MoITT/ PTA`s information However, temporary connection can be made only in necessary situations and the connection must be protected by firewall and segregated from MoITT/ PTA`s network to prevent any threat.

OS_9. If any mobile device is lost or stolen, the Security Manager of the concerned MoITT/ PTA and law enforcement MoITT/ PTA (like Police, FIA etc must be intimidated immediately).

OS_10. There must be emergency plan(s) for purge, physical destruction, self locking, remote wiping of data and self destruct incase of compromise to mobile device(s).

4.12 Physical Security

4.12.1. Policy Objective

This section describes criminal access, physical damage, sabotage, unintended use, and illegal interference in MoITT/ PTA`s information & computer system(s).

This section of the policy deals with the prevention of unauthorized/ criminal physical access, damage to system(s) and illegal interference to the MoITT/ PTA`s premises and information systems.

4.12.2. General Controls

In order to maintain physical security, MoITT/ PTA are to ensure that:

PH_1. Establishment and safeguarding of physical placement of system is determined solely upon the assessment of risk. Such risk assessments can be carried out during construction phase of a new system or risk assessment of existing workspace.

PH_2. Physical space must be "Zoned" as per their security requirement and each of these zones must be designated specific security level. Generic classification of security levels is given in table below:

Security Level	Description
Minimum	This security level is designated to the areas/ assets which have no classification. Unsuitable for non-public government operations
Baseline Protection	This area contains the control assets and information

	having moderate to low security
Medium Protection	This area contains the control assets and information having medium security
High Protection	This area contains the control assets and information having HIGH security

PH_3. Each zone must be equipped with appropriate physical security controls implemented by the MoITT/ PTA.

PH_4. Strict compliance to "Clean Disk" and "Clear Screen" policies.

PH_5. Rooms where MoITT/ PTA`s servers are installed must be having at least MEDIUM protection classification/ level.

PH_6. Network cable(s) (Cat-VI, Coaxial or Optic Fiber) which carry information of level C1 to C3 are to be separated physically and are to be laid in separate ducts.

PH_7. Standard Operating Procedures along with Site`s Security Plan must be prepared for secure system areas. This plan must include the following information:

- Brief summary of security risks assessment,
- Roles and responsibilities criteria/ duties of MoITT/ PTA`s Security officer and other sub-ordinates,
- Supervision, maintenance/ operation of electrical & electronic and mechanical systems, location & working of CCTV camera(s) and working of security/ fire alarm system,
- Fire suppression systems,
- Security & management of key box,
- Adding and exclusion of system user(s) and assigning of personal/ unique identification to such users,
- Security clearance of MoITT/ PTA employees, arrangement of briefings and training sessions regarding security awareness,
- Review of inspection and audit points,
- Lockup of offices at the end of working day, and

- Log of security breaches and incidents.

4.13 Virtualization

4.13.1. Policy Objective

Security of virtualized Information Technology Infrastructure of an MoITT/ PTA is discussed in this section. Great emphasis is laid over MoITT/ PTA`s virtualized environments security.

14.13.2 General Controls

In order to ensure a secure virtualized environment, an MoITT/ PTA must:

VL 1. Virtual technologies and risks associated to it.

- Fore sighting the potential risks in aspects of legal domains, regulatory policy and national legislation procedures.
- Evaluation of impact of virtual technology over its current information technology infrastructure and risks rising in this context.

VL2. Implement hardening of all components of virtual machines and their related services according to the industrial standards, best practices followed around the world and as per vendor`s specifications/ recommendations.

VL3. For managing the virtual environment, least and separation of duties among staff arranged so:

- Define scope, duties, roles and privileges of each administrator/ supervisor who deals with Virtualization Management Software (VMS),
- Containing and limiting direct access to hypervisor up till possible limits,
- Multifactor authentication must be applied as per classification of information and potential risks of virtualization. Also control must be split into multiple administrators.

VL4. Applying of robust security at physical level to prevent any illegal or unauthorized access MoITT/ PTA`s virtual technology environment.

VL5. For security of virtualized technology environment on model of "Defence In Depth" approach, third party security technologies must be incorporated to create a layered security environment.

VL6. Segregation and classification of virtual machines on the nature of data/ information these machines contain or process.

VL7. An enhanced and automatic change management process which ensures that:

- Updation of virtual machine profile and check of its integrity all around the clock,
- Dormant and offline virtual machines` log must be maintained too.

VL8. Activity and other logs generated by the virtual machine`s environments must be properly check and monitored in parallel with logs generated by other information technology equipment.

Chapter - 5

Personal Information Protection
Law of the State of Pakistan

5.1 General Provisions

Article1: Personal information protection law is endorsed in accordance with Constitution of Pakistan to safeguard & reasonable use of the personal rights and information of Pakistan`s citizens.

Article2: Information of an identifiable individual which is recorded/ stored by electronic or other means is defined as "**Personal information**". This definition excludes the information gathered through anonymous means. While processing of personal information includes collection, use, storage (temporary or permanent), transmission, and erasure.

Article3: This law is applicable on personal information processing within the territorial boundaries of Pakistan. However this law is applicable outside Pakistan` boundaries on processing of personal information under following circumstances:

- When the sole purpose of the information is to provide services and/ or products to Pakistani individuals,
- When the sole purpose is to monitor the activities of Pakistani individuals and further these are to be analyzed and evaluated, and
- When it is requested by/ provided with circumstances by laws and other administrative and legislative regulations.

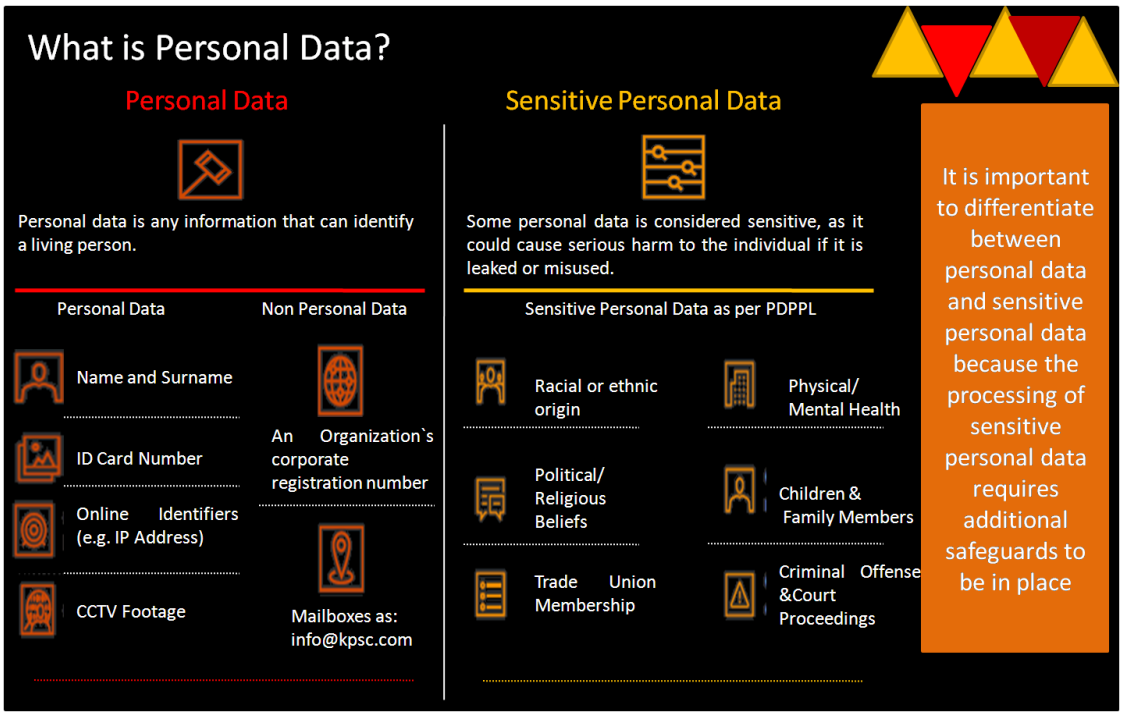

Figure 5.1: Personal Information

Article4: Law shall always safeguard the Personal information of individuals and other entities (either an organization or another individual) will not be allowed to interfere in rights and personal information.

Figure 5.2: Data Privacy and Organization

Article5: While processing of personal information, due care and commitment must be observed. Good faith and other moral principles must be followed and malpractices must be avoided.

Article6: There must be a clearly definite and reasonable purpose for processing of personal information and this must be done in way which throw as little as possible effect on interests and rights of an individual. Collection of information must be as per requirement and collection of unnecessary information must be avoided.

Article7: There must be openness and transparency during the process of information collection and processing; and explicitly express the manner, scope and purpose of the information processing.

Article8: Quality of the information, while it is being collected must be ensured for correctness and it must not put adverse affects over individual rights and interests due to incorrectness and incompletion.

Article9: The person who will process the information shall be fully responsible for it and will have to take necessary steps and measures for the integrity and security of the processed information and results deduced from it.

Article10: Collection, processing, trade, use, and transmission of personal information by an individual or organization in illegal way will never be allowed which may result in endangering personal or national security interest.

Article11: State will establish a comprehensive system for personal information protection in order to prevent the spill of information and subsequent infringement. This system will also promote a sound environment for the joint and collective effort by all the institutions of Pakistan for security and protection of personal information.

Article12: State will participate actively in process of formulation of ruling for protection of personal information on international law. This formulation must also cover international level exchange of data and mutual recognition of set rules on international levels including territorial regions and international organizations.

5.2 Rules Governing Processing of Information

Section 1: General Provisions

Article13: Personal information will be process only in following circumstances:

- After consent of individual whose data is going to be processed,
- When the individual concerned is a member of an agreement and term as a party; or when Human Resource Management (HRM) is implying any labor rule,
- When it is required for statutory obligations and duties related performance,

- When such information is necessary for public interest and information processing is in reasonable and legitimate scope,
- When individual discloses his/ her personal information or by other legally allowed individuals and it is in harmony with provision of personal information protection law, and
- Any additional circumstances/ contingencies chalked out by administrative and legislative regulations and laws.

Article14: While approval of individual is being taken for information provision, this consent must be taken voluntarily and there must be no coercion over the individual. Explicit and full knowledge to the individual must be provided. If the consent is required in written, it must be produced to the law and regulation entity which is demanding the said. If the purpose/ utilization of information changes, the consent must be taken again.

Article15: If concerned individual is minor/ less than 15 years of age, consent must be obtained from minor`s parent(s) or guardian. There must be specific rulings for processing of minor`s information devised by the concerned department.

Article16: If an individual withdraws his/ her consent or does not agree on sharing of personal information, information processor won`t refuses to provide services and will arrange convenient means for withdrawal.

Article17: Before commencement of information processing, information processor must inform the individual in a truthful, accurate and straight manner the following matters in clear and in language which is understandable by the individual:

- Name and contact number of the person who is going to process the information,
- Method which will enable the individual to use his/ her rights,

- The purpose for which the information is required and method which will be followed during process, and
- Any other issues that are in accord with provision(s) of administrative regulations and laws.

Upon occurring of change in any provision, individual must be notified and properly informed of that change.

Article18: During process of information, information processor will not let the individual know where confidentiality has to be maintained in matters where law and administration regulations are concerned.

Article19: Personal information must be retained for the shortest possible time necessary for processing or for specific duration set by concerned law and administration regulations.

Article20: In case of joint processing of data by couple of processors or more, together and they jointly determine the method of processing information, they must agree upon the respective rights and obligations. However, this will not affect the right of an individual to exercise protection of his/ her personal information against any particular information processor.

In case any infringement happens during joint processing of personal information which cause damages, all personal information processors shall jointly bear the burden and liabilities.

Article21: When there develops a mutual trust between two personal information processors, they are to agree upon processing, protection measure and type as well as obligations and rights of both parties involves. Further the personal information processing will only be carried out till the limit set by mutual consent of the parties and

not beyond it in all case and upon cancellation of contract, invalidation or revoking, the entrusted partner must either handover back the personal information of the client or remove it. In any case the entrusted partner will not retain with it the personal information of the individual and entrusted partner will never re-enter with other personal information processors.

Article22: If an information processor is unable to carry out processing (for reasons like, merger, dissolution or becomes bankrupt); he/ she will transfer the complete information of individual(s) like name, phone number and other information to the recipient (another processors which are involved in processing) who shall continue the personal information processing ahead and will be abide by all obligations. The recipient will inform the individual (whose information is being processed) and if recipient changes the method and original purpose of information processing and must obtain consent of individual in this regard.

Article23: If a personal information processor shares the personal information of individual(s) with another information processor, he/ she must let the particular individual know and will take individual`s approval. Processor of personal information must share the complete information of information processor like name, phone number and method of processing and shall get consent from the individual. If receiving party changes the method and original purpose of information processing and must obtain consent of individual in this regard.

Article24: Transparency, justice and fairness must be ensured while automatic decision making is applied during personal information processing and there must not be any discriminatory or differential treatment of individuals involved.

While marketing of business and promotions are carried out using automatic decision making, personal characteristics must not be provided for choice and individuals must have right to reject the options offered.

An explanation from personal information processor may be asked if there comes considerable impact on individual`s rights, interests & stake during automatic decision making.

Article25: Any personal information that is being process, processor shall not disclose it in any case. However he/ she could do so with the consent of individual or per requirement of law & administrative regulation(s).

Article26: Any device and equipment which is capable of capturing individual`s imaging identity (for example, camera in a public place) will be employed for uphold public security; must strictly adhere to relevant laws set by Government of Pakistan. These captured images must only be used for their intended purpose and if needs to be used in some other work, consent from individual must be taken.

Article27: Personal information of the particular individual can be disclosed within a reasonable range, like the information individual has shared by his/ her own and lawfully disclosed. Prior to disclosure of personal information, personal information processor must take prior consent from the concerned individual(s) in accordance with laws if the disclosure has a foremost impact on rights and interests of individual .

Section 2: Declared Rules for Processing of Sensitive Personal Information

Article28: Any information of an individual which, if released, can damage, cause infringement in the personality, cause security risk or prove harmful to the life and property of an individual is declared as “Sensitive Personal Information”. This sensitive information includes unique identities, religious beliefs, political affiliation, financial

details, biometric identities and medical health; and personal information of minors whose age is under 14.

Personal information processor must process these sensitive identities only when required and with great care and diligence.

Article29: Personal information processor must take consent of individual must be taken before processing his/ her sensitive personal information, and where law requires; the consent may be taken into written form.

Article30: Personal information processor must inform the individual whose sensitive personal information he/ she is going to process; also inform individual of impact on his/ her interests and rights.

Article31: Personal information processor must know that he/ she is processing the sensitive personal information of a minor (who is below 14), processor must obtain consent for processing such sensitive data from minor`s parent or guardian. Personal information processor must formulate the policy and regulation for processing minor`s sensitive information.

Article32: During the process of sensitive personal information processing of any individual is ordered by law and administrative regulation, sensitive personal information must be processed if law grants provisions to do so.

Section 3: Role of State Organs and Special Provisions

Article33: Activities of a state organ regarding processing of personal information, this law shall be applied. Where there are specific provisions in particular section, the provisions of that section will be applied.

Article34: When a State organ processes personal information for performing its statutory duty, its processing activity must be observed and governed by the prescribed laws and liabilities and the information processing activities of that state organ shall not exceed the legitimate limits.

Article35: A State organ, processes personal information for performing its statutory duty, shall abide to laws, obligations and regulations set by Government of Pakistan except for extreme circumstances described in **Article: 18**. Government can too hinder a state organ from performing processing task by issuing a notification.

Article36: All the personal information which state organ process must be kept stored withinin Pakistan. Security assessment with the help of relevant department shall be conducted prior to handing the process information to overseas partner(s).

Article37: This law enables state organs to apply to other personal information processors and organizations for processing of personal information on its behalf. Such hiring of organization must be carried out under laws and regulations enforced in parallel with managing public affairs and performing statutory duty.

5.3 Rules Governing Cross-border Provision of Personal Information

Article38: Whenever an information processor is required to make available processed personal information to entities outside territorial boundary of Pakistan (amid any circumstances), it shall have to fulfill the following conditions:

- Where the organization with which the processor is going to share the information has passed the security assessment criteria set by Pakistan`s MoITT / PTA

- With respect to protection of personal information of an individual, has the concerned company is specialized in standards in accordance with MoITT / PTA
- While concluding information sharing agreement with overseas organization has the personal information processor followed the rules and criteria set by MoITT / PTA and obligations & rights of both the parties are fully specified
- Any provision which has been concluded between state of Pakistan and international organization earlier regarding sharing of personal information has added to the contract

Article39: Any individual whose data is being shared with international organization(s) or outside Pakistan; he/ she must be informed of such sharing along with details of entities with which will be receiving the data. Individual must also be informed about his/ her right against the foreign recipient and obtain consent from Individual.

Article40: When personal information processing by Critical Information Infrastructures & Personal Information Processors reaches the permissible level set by Government of Pakistan; they must store their processed information within state of Pakistan. If this information has to be shared with foreign partners, it must be done after security assessment described by MoITT / PTA.

Article41: Any request made to Pakistan by foreign country`s law enforcement or judicial MoITT/ PTA for provision of personal information processed and/ or stored in Pakistan; competent cyber authorities of Pakistan shall act in accordance with laws, regulations, treaties, accords and international agreements. Without the approval of MoITT / PTA, the requested information must not be provided to the foreign entities.

Article42: Any foreign organization whose activities w.r.t processing of personal information damage the Pakistani citizen`s rights pertaining to personal information, endangers national integrity, security and stability of Pakistan; then MoITT / PTA may blacklist that particular foreign organization and prohibit sharing of information with it.

Article43: When any country, foreign organization or region gets committed in negative activities and measures against Pakistan w.r.t protection of personal information; then Pakistan reserves the right to take reciprocal measures against such entities.

5.4 Individual Rights in Activities of Processing Personal Information

Article44: All individuals/ data subjects are entitled with full right to remain aware and make decision about their personal information and right to bar the access to this information, depending upon the rules and regulations put forward by administrative and law departments.

Article45: Individuals are fully entitled to obtain copy of their personal information directly from the processor of their personal information; subject to the situations described in **Article 18** and **Article 35**. Upon reception of this request, information process is liable to provide requested information timely.

When information transfer request is pleaded by an individual for transfer of his/ her personal information to another processor designated by the individual; the information processor who was processing the information shall arrange smooth transfer of information to the newly nominated information processor in accordance with laws and regulations imposed by MoITT/ PTA.

Article46: Upon finding some incorrectness, ambiguity or incompleteness in personal information, individual is entitled with right to plead for correction of information.

Upon receiving of alteration/ correction request, personal information will make required correction in timely manner once the individual identity verification is completed.

Article47: Personal information which is held with the personal information processor can be deleted upon request of the individual. Also the information processor can delete the information of any particular individual but for doing so information processor has to fulfill following conditions:

- When the objective of processing is achieved or failed to achieve or the information is no longer required,
- When the product support from personal information processor is terminated or agreed duration for storage has expired,
- Upon withdrawal of individual`s consent,
- When personal information processor, while processes the information violates any law of administrative, regulation or agreement clause, or
- Any other circumstances/ condition described by the administrative regulations and laws.

When the storage period is not expired and deletion of personal information is not feasible, then the processing of that particular personal information must be halted.

Article48: An individual has right to ask personal information processor for explanation of the rules under which processing of his/ her personal information is being carried out.

Article49: In case if the individual`s death, all rights of individual`s personal information will be automatically transferred to his her relatives or next of kin, unless information will be treated per decisions prior to the individual`s demise.

Article50: All personal information processor are liable to impose an easy and convenient mechanism for reception, processing and outcomes of applications regarding individual`s personal rights, if personal information processor rejects the said application(s); he/ she will have to state the reason.

If personal information processor rejects the application of an individual regarding exercise of his/ her rights without stating reason, individual can file a lawsuit against that particular personal information processor according to law in people`s court.

5.5 Obligations Related to Personal Information Processors

Article51: All personal information processors will follow the obligations/ principles given below according to the information`s nature, type, its impact over individual rights, well being & interests, and the method with which the information will be processed:

- Devising and formulation of integrated internal management, application processing and official operational set of procedures,
- Management/ organization of personal information on its classification,
- Considering and implementing technical as well as security measures (like cryptography, encryption etc) for integrity and security of information,
- Determination of authority w.r.t processing of personal information and conduction of training and likewise security education for its` employees on regular basis,
- Formulation of emergency and likewise contingency plan(s) against security threats to personal information, and
- Adhering to other laws prescribed by administrative regulations and laws.

Taking of the above mentioned measure will guarantee the compliance of personal information processing under the umbrella of regulations & laws and if followed perfectly, these provisions will prevent leakage, compromise and/ or loss to the personal information.

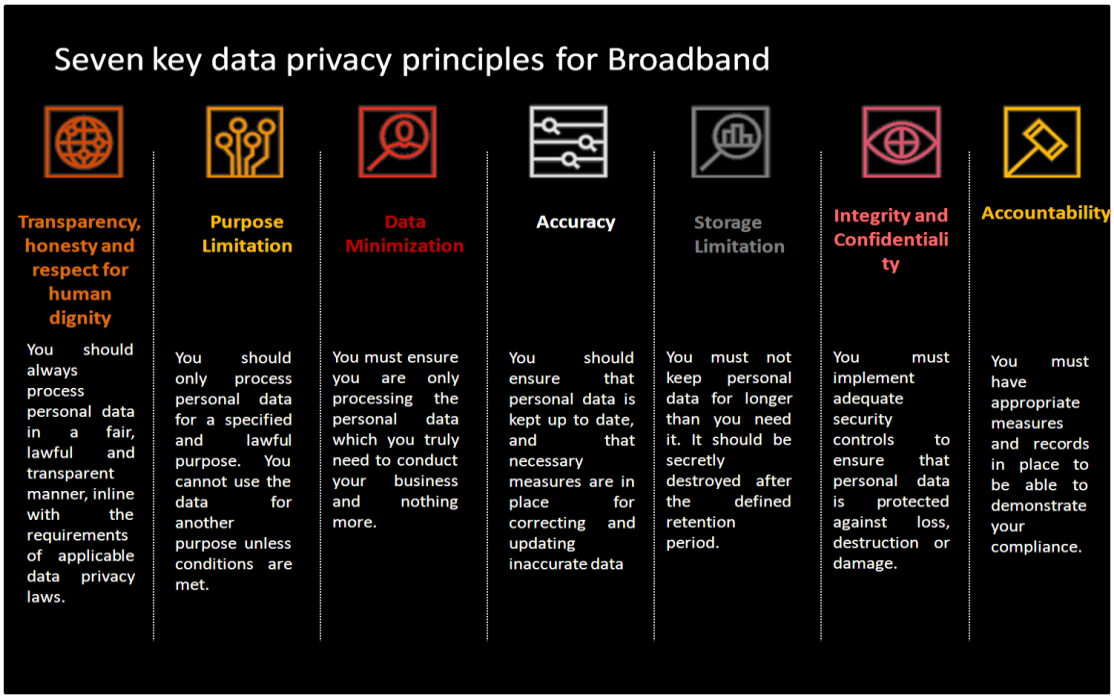

Figure 5.3: Seven Key Data Privacy Principles

Article52: Upon reaching a prescribed limit (set by MoITT/ PTA) of personal information processing, personal information processor will be responsible to designate a person who will be fully responsible for protection of this information and will supervise the processing of personal information at all stages and will adopt the every possible security measure.

A processor of personal information will disseminate credentials (name(s), contact number) of person in charge with the individual(s) and authorities concerned.

Article53: The personal information processor(s) who are situated outside territorial boundaries of Pakistan (prescribed in **Article 3**) shall designate a special representative, either an individual or organization within Pakistan. This representative will be accountable for all the related matters regarding protection of Personal Information and its details along with contact numbers will be shared both with individuals concerned and MoITT/ PTA.

Article54: Personal information processor will regularly conduct self audit to check that whether he/ she is complying with the provisions of set forth by MoITT/ PTA while processing the personal information or not?

Article55: A personal information processor will be liable to conduct information impact assessment subject to given circumstances and will maintain a proper record of it:

- Processing of sensitive personal information(s),
- Automatic decision making using personal information,
- Sharing of personal information of individual(s) with other personal information processor(s),
- Sharing of personal information with overseas organizations/ parties, and
- Information processing activities that impact significantly over individual rights and interests.

Article56: Impact assessment of personal information processing must contain the following:

- Is the processing of personal information is legitimate, morally & legally justifiable and necessary?

- How this processing of personal information is going to impact an individual`s rights, his/her interests and security risk associated to him/ her?
- Are the security & protection measures adopted during personal information processing are efficient, effective, legitimate and appropriate to the degree of risk(s)?

Article57: All necessary and remedial measures must be taken by the personal information processor as soon as there is report of leak, theft, compromise or falsification of personal information and the department which is governing duties of personal information protection must be informed along with the individual(s) concerned. The notification must contain:

- Cause of information leakage, its nature and possible threats the leak may pose to the concerned individuals.
- Remedy actions taken by the personal information processors and individual(s) concerned to mitigate the harm(s) posed by security breach.
- Contact information (mobile, landline & email) of personal information processor(s).

If the measures taken by the personal information processor effectively counter the threat posed by leak and mitigates it properly; the processor of personal information may opt not to inform/ let the individual(s) know whose data was compromised.

If the department which is governing the duty of protection of personal information believes that harm is likely going to cause, it may order personal information processor to inform the individuals concerned regarding compromise to their data.

Article58: The personal information processor which provide internet services and having large customer base, or business entities which are involved in complex business practices must adhere to the obligations mentioned below:

- Establishment and improvement of a compliance system which will regulate the personal information processing in accordance with laws and regulations imposed on it. It will too be the responsibility of personal information processor to establish a committee for protection of personal information which will consist of external member,
- Formulation of the rules of personal information processing setup which must adhere to the norms of fairness, openness, justice, clearly stating norms for personal information processing, and obligations of service provider within the organization to protect the individual`s personal information,
- Barring of service or support to the users who are involved in serious abrogation of laws and regulations during process of personal information, and
- Releasing report on social responsibility of the personal information processor on regular basis.

Article59 Any party which is given to process personal information must fulfill the requisite obligations described in this law along with other relevant administrative regulations and laws, must adopt necessary measures to keep secure the processed personal information their obligations/ adherence to the laws.

5.6 Departments Performing Duties of Personal Information Protection

Article60: It will be the responsibility of MoITT / PTA to coordinate, supervise and regulate the protection of personal information. Responsibility of relevant departments

under the control of Pakistan will be to protect, supervise and administer the personal information within their orbit of responsibility & scope and in full adherence to laws and regulations imposed by government.

The departments which are described in above mentioned couple of paragraphs are combined referred as the departments which will safeguard the personal information and will perform duties of protecting the information against any malicious and illegal activity.

Article61: Following are the responsibilities of the departments which will be dealing with personal information protection:

- To carry out publicity, provide guidelines and educate/ promote awareness regarding personal information`s protection to its processors,
- Acceptance as well as swift process of complaint mitigation regarding protection of personal information,
- Carrying out evaluation of the protection mechanism of personal information and generate its results,
- Investigation and subsequent processing of illegal access activities to personal information processing domains, and
- Any additional duties stipulated by administrative regulations and laws.

Article62: MoITT/PTA shall remain in constant coordination with relevant departments for promoting and imparting utmost protection of personal information in harmony with following laws:

- Formulation of specified rules and setting of standards in domain of protection of personal information,

- Formulation of particular rules and setting of standards in domain of protection of personal information by small sized personal information processor, and implementation of new technologies (like face recognition) and applications (like artificial intelligence),
- To support the subordinate personal information processor in research, development and secure authentication technology for security and services which can facilitate individual(s) online identification,
- Carrying out assessments and certification services (on the basis of assessment carried out) of the organizations and making a socialized service system for personal information`s protection, and
- Improvement in the mechanism for addressing whistle-blowing and complaint management of personal information processing.

Article63: Department which are assigned with the duties of personal information protection by MoITT/ PTA must consider following points:

- Thorough check, inquiry and investigations of parties concerned and circumstances regarding activities of personal information processing,
- Audit and copying of all contracts, account ledgers, contracts and other relevant documentation regarding activities of parties concerned in personal information processing,
- To rule out the suspected violation of laws relating personal information processing, carrying of spot and on-site inspections and related investigations,
- If there found trace of any illegal activity or activities carried out by the personal information process, his/ her articles, devices and systems may be confiscated after written application to the principal of governing department and subsequent approval, and

- The parties which are concerned with the personal information processing must fully cooperate with the superior departments in accordance with laws and regulations of Government of Pakistan i.e MoITT/ PTA and must not refuse to provide assistance.

Article64: In case of occurrence of any incident related to personal information processing or if high risk during processing or other related security risk, processor of personal information may take an interview of the individual concerned or his/ her legal representative as per mentioned by the governing authority.

Personal information processor shall ensure to make rectifications, identifications and elimination of hidden dangers and potential threats in personal information repository as per requirements.

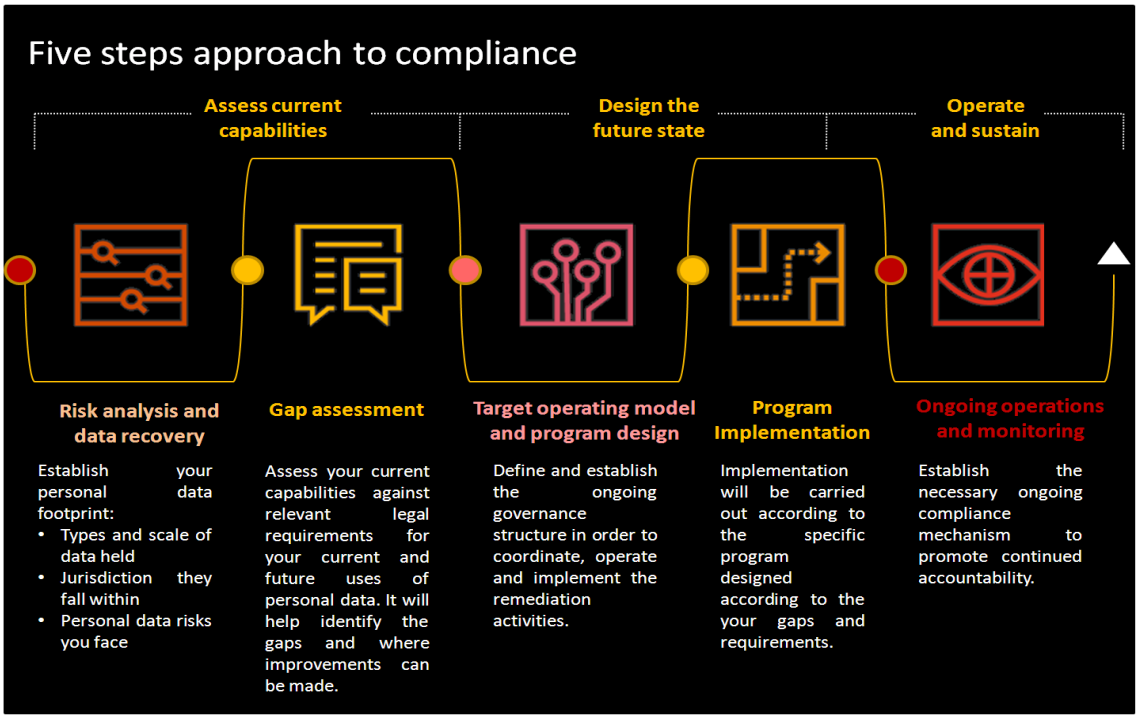

Figure 5.4: Five Step Approach to Compliance

If a personal information processor is found involved in processing of personal information illegally or is suspected of committing a crime during performing duty; the department concerned must transfer the said criminal case to the security organ which is responsible for the security of personal information.

Article65: Every organizations as well as individuals are entitled with right to lodge complaint against illegal processing of personal information and related malicious activities. Upon reception of such complaint(s), concerned departments will promptly process the application according to issued it is related and further will notify the process, finding(s) and result(s). For ease of entities in lodging complaints, the departments must make sure their contact details are publically available.

5.7 Legal Liability during Personal Information Processing

Article66: If personal information is processed against the defined provisions and laws, or the personal information is processed without adhering to the rules & regulations defined here, the department will warn the processor; take away illegal gains obtained from information processing, suspension/ termination of services from the information processor and make rectifications. In case rectification is refused to be done, fine (less than PKR 1 million) will be charged on the processor. A fine ranging in between Ten Thousands to Hundred Thousands Rupees will be imposed on the individual in charge of the information processor(s) and other individuals who are directly involved in processing process. When an illegal act as per described in earlier paragraph, is committed and the circumstances and extraordinary & serious, the department confiscate illegal gains obtained from information processing and impose fine less than PKR 50 million or at least five percent (5%) of its turnover of preceding year. Concerned department may too order the information processor to suspend/ cease its business activities for rectification and revoke the license and other relevant business permits along with a fine in between PKR 100,000 and 1,000,000 on the individual

directly handling the information processor and/ or other individuals who are directly involved. Such culprit person(s) may be prohibited/ blacklisted from serving on any key position(s) like directors, senior managers (both administration and/ or operations) for a specified duration of time.

Article67: Any sort of illegal act which is defined in this law, must be properly recorded along with credit archive(s) as per provisions of the relevant state law and per reference with the regulations must be made available to the public.

Article68: When a state organ could not fulfill its role in protecting personal information and fails to perform the obligations pertained to it, the superior state organ will order the particular sub-ordinate organ for making rectification(s) and will enforce sanctions on that particular person(s) of that organ who failed to fulfill their duties as per law and regulations devised by MoITT/ PTA.

When the staff member(s) of the departments (which are responsible for protection of personal information) are found involved in abusing of their official powers, doing malpractices or doing illegal activities for their personal gains but have not constituted a crime, they must be given punishment as per law and regulations of Pakistan`s cyber world.

Article69: If there occurs an infringement or compromise to the personal information while it is being processed and subsequently causes damage(s) and the personal information processor fails to prove its occurrence due to fault, he/ she will bear the full liability of the damage occurred.

The liability of damage which is discussed in earlier paragraph must be borne by the personal information processor w.r.t the loss caused to the individual or the benefit(s) availed by the processor of personal information, if this loss or gain is difficult to be

determined, then the public court shall be consulted to determine the compensation and amount to be paid, keeping in view the actual circumstances.

Article70: When a personal information processor violate the provision of this law while processing individual`s personal information, and this violation results in compromise to the rights and interests of individuals whose information was held with the above mentioned personal information processor; then the people`s protectorate department and/ or MoITT/ PTA (which are determined by the MoITT/ PTA) will file the lawsuit/ case against that personal information processor.

Article71: When infringement of the provision of these laws it will results in subsequent breach of public security, punishment shall be imposed on it as per description of law and if a crime is held, a criminal charge shall be investigated in proper accord with the laws and regulations chartered by the MoITT / PTA.

Chapter - 6

Conclusion and Future Work

6.1 Conclusion

Broadband world expansion and our reliance over it will ever prevail and threats related to it will ever rise too. This expansion will come too with new demands and challenges which will need to be addressed and formulation of laws for countering broadband world related crimes. Said objectives can only be achieved by implementation of National Broadband Policy [NBSP V1.0] in its true essence. Further addition of laws and refinement of current provisions in broadband policy is going to be time saving, more productive and efficient. Nature of this policy is very flexible thus any addition to its laws in relation with new threats; will enhance its efficacy in divers environments of broadband world.

6.2 Future Work

In the proposed National Broadband Policy [NBSP V1.0] framework, following domains are open for future research and enhancement:

- Formulation of new laws which counter new broadband world related threats and crimes and incorporation of those laws in National Broadband Policy [NBSP V1.0] as informative reference.
- Identification techniques of broadband related threats addition of these techniques in National Broadband Policy [NBSP V1.0].
- Integration of Broadband domain protection techniques.
- Methodology for recovering of lost data due to broadband world crimes.
- Development of broadband crime detection methodology/ techniques and its amalgamation in National Broadband Policy [NBSP V1.0].

References :

[1] https://www. qcert.org

[2] https://www.china-briefing.com

[3] https://www. qcert.org

[4] https:// en.wikisource.org

[5] https:// www.dataguidance.com

[6] www.sa.gov.au

[7] "African Data Privacy Laws", Springer Science and Business Media LLC, 2016

[8] www.lapres.net

[9] uwspace.uwaterloo.ca

[10] www.coursehero.com

[11] www.phoneworld.com.pk

[12] www.gcsb.govt.nz

[13] www.motc.gov.qa

[14] Xu Junke, Tang Ying. "Legal Protection of Personal Data in China", 2021 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), 2021

[15] www.pta.gov.pk

[16] www.privacy.gov.ph

[17] www.nzism.gcsb.govt.nz

[18] "Data Protection Around the World", Springer Science and Business Media LLC, 2021

[19] www.national.archives.gov.za

[20] "The Handbook of Privacy Studies", Walter de Gruyter GmbH, 2018

[21] Binxing Fang. "Cyberspace Sovereignty", Springer Science and Business Media LLC, 2018

[22] blog.ipleaders.in

[23] security-guidance.service.justice.gov.uk

[24] David Slee. "The data protection bill 1998: A comparative examination", Information & Communications Technology Law, 1999

[25] Pavol Sokol, Radoslav Benko, LauraRózenfeldová. "Chapter 13 Legal Issues of Deception Systems in the Industrial Control Systems", Springer Science and Business Media LLC, 2020

[26] hdl.handle.net