

1. What do you mean by digital signature? Write the role of controller of certification authority according to Electronic Transaction Act, 2063.

→ A **digital signature** is an electronic method used to verify the authenticity, integrity, and non-repudiation of digital messages or documents. It is created using **asymmetric cryptography**, where the sender signs a document with a **private key**, and the recipient verifies it using the corresponding **public key**. Digital signatures ensure that the message has not been altered and confirm the identity of the sender.

Role of Controller of Certification Authority (CCA) According to Electronic Transaction Act, 2063

As per **Electronic Transaction Act, 2063 (2008)** of Nepal, the **Controller of Certification Authority (CCA)** is responsible for regulating and supervising digital certification authorities (CAs). The key roles of the CCA include:

1. **Licensing of Certification Authorities (CAs)** – The CCA grants licenses to CAs for issuing digital certificates.
2. **Monitoring and Supervision** – Ensures that CAs operate according to the set guidelines and security standards.
3. **Revocation or Suspension of Licenses** – Can revoke or suspend the license of a CA if they violate the law.
4. **Setting Standards for Digital Signatures** – Defines cryptographic and security standards for digital signatures.
5. **Verification and Audit** – Conducts periodic audits and inspections of CAs to ensure compliance.
6. **Handling Disputes** – Resolves conflicts related to digital signatures and certificate usage.
7. **Public Awareness and Promotion** – Promotes the use of digital signatures for secure electronic transactions.
8. **Maintaining a Repository** – Keeps records of all issued, revoked, or suspended digital certificates.

These roles help maintain trust and security in electronic transactions in Nepal.

2. Write any five strategic policy of ICT policy, 2072.

→ The **ICT Policy, 2072 (2015)** of Nepal outlines several strategic policies to promote the development and use of Information and Communication Technology (ICT) in the country. Here are **five strategic policies** from the ICT Policy, 2072:

1. **Expansion of ICT Infrastructure** – Ensure widespread access to ICT infrastructure, including broadband internet, data centers, and communication networks in rural and urban areas.
2. **Promotion of E-Governance** – Implement e-governance systems to enhance transparency, efficiency, and accessibility of government services through digital platforms.
3. **Development of ICT Industry** – Support and encourage local ICT industries, startups, and innovation centers to strengthen Nepal's digital economy.
4. **Cyber Security and Data Protection** – Establish legal frameworks and security measures to safeguard digital transactions, personal data, and national cyber infrastructure.
5. **Human Resource Development in ICT** – Develop skilled manpower in ICT through education, training programs, and research initiatives to increase employment opportunities in the IT sector.

3. What is Cyber law? What does the cyber law incorporate? Why cyber law is necessary?

→ **Cyber law** refers to the legal framework that governs activities conducted over the internet and digital platforms. It includes laws related to cybercrimes, electronic transactions, data protection, intellectual property rights, and digital security. Cyber law helps regulate online behavior and ensures the lawful use of technology.

What Does Cyber Law Incorporate?

Cyber law covers various aspects of digital activities, including:

1. **Cybercrime Prevention** – Laws against hacking, identity theft, phishing, cyber fraud, and online harassment.
2. **Electronic Transactions** – Regulations for digital contracts, electronic signatures, and online business transactions.
3. **Data Protection and Privacy** – Legal provisions to protect personal and sensitive data from misuse.
4. **Intellectual Property Rights (IPR)** – Protection of copyrights, trademarks, and patents in the digital space.
5. **Cybersecurity and Network Protection** – Guidelines for securing networks, preventing cyber threats, and ensuring national security.
6. **Regulation of Digital Content** – Monitoring of illegal content, including fake news, cyberbullying, and digital piracy.

Why is Cyber Law Necessary?

Cyber law is crucial for the following reasons:

- ✓ **Prevents Cybercrime** – Protects individuals and organizations from hacking, fraud, and cyber threats.
- ✓ **Ensures Privacy and Security** – Safeguards personal and financial data from misuse.
- ✓ **Regulates E-Commerce** – Provides a legal framework for secure online business transactions.
- ✓ **Protects Intellectual Property** – Prevents unauthorized use and distribution of digital content.
- ✓ **Supports Digital Governance** – Helps governments implement e-governance and provide secure online services.
- ✓ **Establishes Legal Accountability** – Holds individuals and organizations accountable for online activities.

Cyber law is essential in today's digital world to ensure a safe, secure, and trustworthy online environment.

4. Explain briefly the major component of the existing cyber law and copyright Act of Nepal.

→ Major Components of the Existing Cyber Law and Copyright Act of Nepal

Nepal's cyber law is primarily governed by the **Electronic Transaction Act (ETA), 2063 (2008)**, while intellectual property rights, including copyright, are regulated by the **Copyright Act, 2059 (2002)**. Here are the key components of both laws:

1. Major Components of the Electronic Transaction Act (ETA), 2063 (2008)

The **Electronic Transaction Act (ETA), 2063** is Nepal's primary cyber law that regulates digital transactions, cybercrimes, and data security. The major components include:

1. **Legal Recognition of Electronic Transactions**
 - Recognizes digital records, electronic signatures, and online contracts as legally valid.
2. **Regulation of Certification Authorities**
 - Establishes a **Controller of Certification Authority (CCA)** to monitor and license Certification Authorities (CAs) for issuing digital certificates.

3. **Cybercrime and Punishment**

- Defines various cybercrimes like hacking, unauthorized access, identity theft, phishing, and online fraud.
- Prescribes penalties such as fines and imprisonment for cybercrimes.

4. **Privacy and Data Protection**

- Prohibits unauthorized access, modification, or disclosure of digital data.
- Ensures the protection of personal and financial information.

5. **Computer and Network Security**

- Imposes legal obligations on individuals and organizations to ensure cybersecurity.
- Penalizes those involved in cyberattacks, malware distribution, and denial-of-service (DoS) attacks.

6. **Content Regulation and Censorship**

- Prohibits the publication or transmission of illegal, offensive, or defamatory content online.
- Penalizes online hate speech, child pornography, and cyberbullying.

7. **Electronic Payment and E-Commerce Regulation**

- Establishes legal provisions for secure online transactions and digital banking.
- Ensures consumer protection in e-commerce activities.

2. **Major Components of the Copyright Act, 2059 (2002)**

The **Copyright Act, 2059** protects intellectual property rights related to creative works. The major components include:

1. **Protection of Creative Works**

- Grants copyright protection to literary works, music, films, software, art, and other intellectual creations.

2. **Rights of Copyright Holders**

- Provides authors and creators with **exclusive rights** to use, distribute, and sell their works.

- Allows them to claim ownership and receive financial benefits from their works.
 - 3. **Fair Use and Limitations**
 - Allows limited use of copyrighted materials for education, research, and public interest under **fair use provisions**.
 - 4. **Copyright Infringement and Penalties**
 - Penalizes unauthorized reproduction, distribution, or modification of copyrighted materials.
 - Includes fines and imprisonment for copyright violations.
 - 5. **Software Copyright Protection**
 - Recognizes software as a protected work and prohibits unauthorized duplication and distribution.
 - 6. **Establishment of Copyright Registrar's Office**
 - Manages copyright registrations, resolves disputes, and enforces copyright laws in Nepal.
-

Conclusion

Both the **Electronic Transaction Act, 2063** and the **Copyright Act, 2059** play crucial roles in Nepal's digital and intellectual property landscape. The **ETA, 2063** ensures cybersecurity, regulates online transactions, and prevents cybercrime, while the **Copyright Act, 2059** safeguards intellectual property rights and promotes creativity.

5. Explain the salient features of Electronic Transaction Act.

→Salient Features of the Electronic Transaction Act, 2063 (2008) of Nepal

The **Electronic Transaction Act (ETA), 2063** is Nepal's primary cyber law that governs digital transactions, cybercrimes, and electronic records. The key features of the act are:

1. Legal Recognition of Electronic Transactions

- Establishes the **legal validity of electronic records, digital signatures, and online contracts** in Nepal.

- Ensures that electronic documents and signatures hold the same legal weight as physical documents.
-

2. Establishment of Certification Authority

- Introduces a **Controller of Certification Authority (CCA)** to regulate **Certification Authorities (CAs)** that issue digital certificates.
 - Ensures the security and authenticity of electronic signatures.
-

3. Regulation of Cybercrime and Digital Fraud

- Defines various **cybercrimes** such as hacking, phishing, identity theft, and unauthorized access to computer systems.
 - Imposes penalties including **fines and imprisonment** for cybercriminal activities.
-

4. Privacy and Data Protection

- Protects **personal data and sensitive information** from unauthorized access or misuse.
 - Penalizes individuals or organizations involved in **data breaches, online defamation, and cyberstalking**.
-

5. Security of Electronic Communications and Networks

- Establishes legal frameworks to **protect computer networks, databases, and digital transactions**.
 - Criminalizes cyber threats, malware distribution, and denial-of-service (DoS) attacks.
-

6. Regulation of E-Commerce and Digital Payments

- Provides **legal recognition to online businesses and e-commerce platforms**.
 - Ensures **consumer protection in digital transactions and electronic banking**.
 - Prevents online fraud and unauthorized financial transactions.
-

7. Content Regulation and Online Ethics

- Prohibits the publication, transmission, or storage of **offensive, illegal, or harmful digital content**.
 - Penalizes **online hate speech, pornography, cyberbullying, and defamation**.
-

8. **Dispute Resolution and Legal Proceedings**

- Allows **electronic records as evidence** in court proceedings.
 - Establishes **legal mechanisms to resolve disputes related to cybercrime and electronic transactions**.
-

9. **Punishment and Penalties for Violations**

- Imposes strict penalties for cyber offenses, such as:
 - **Unauthorized system access** – Up to **3 years imprisonment** or a **fine of NPR 200,000**.
 - **Hacking or data theft** – Up to **5 years imprisonment** or a **fine of NPR 500,000**.
 - **Publishing obscene content** – Up to **1 year imprisonment** or a **fine of NPR 100,000**.
-

10. **Establishment of Cyber Regulations and Awareness**

- Promotes **public awareness of cyber laws and digital security**.
 - Encourages **government agencies and private organizations** to follow cyber laws for digital safety.
-

Conclusion

The **Electronic Transaction Act, 2063** is a crucial legal framework for **ensuring cybersecurity, promoting digital transactions, and preventing cybercrime** in Nepal. It plays a significant role in protecting individuals, businesses, and government institutions in the digital age.

6. **Briefly explain some salient features of current National ICT policy.**

→ **Salient Features of the Current National ICT Policy of Nepal (ICT Policy, 2072 - 2015)**

Nepal's **National ICT Policy, 2072 (2015)** aims to promote digital transformation, enhance ICT infrastructure, and support economic growth through technology. Some of its key features are:

1. **Development of ICT Infrastructure**

- Expansion of **broadband connectivity, data centers, and cloud computing services** across Nepal.
 - Promotion of **fiber-optic networks and rural telecommunication services** to bridge the digital divide.
-

2. **Promotion of E-Governance**

- Implementation of **electronic government services (e-governance)** for transparency and efficiency.
 - Establishment of **digital identity systems (e.g., National ID, digital signatures)** for secure access to online services.
-

3. **Cybersecurity and Data Protection**

- Strengthening **cyber laws and frameworks** to combat cyber threats and enhance national security.
 - Ensuring **data privacy, secure online transactions, and protection of personal information**.
-

4. **ICT Industry Development and Innovation**

- Encouraging **IT startups, entrepreneurship, and innovation hubs** to boost Nepal's digital economy.
 - Supporting **software development, IT outsourcing, and business process outsourcing (BPO) services**.
-

5. **Digital Literacy and Human Resource Development**

- Integrating **ICT education in schools, colleges, and technical institutions**.

- Providing **skill development programs, scholarships, and training for IT professionals.**
-

6. **Promotion of E-Commerce and Digital Payment Systems**

- Encouraging the use of **electronic transactions, mobile banking, and digital wallets.**
 - Establishing policies for the growth of **online businesses and digital marketplaces.**
-

7. **Research, Development, and Innovation in ICT**

- Promoting **R&D in emerging technologies** like Artificial Intelligence (AI), Blockchain, and Cloud Computing.
 - Encouraging **collaboration between academic institutions, government, and the private sector** in ICT research.
-

8. **Environmental Sustainability in ICT**

- Encouraging the use of **green computing and energy-efficient ICT solutions.**
 - Establishing **e-waste management systems** for the disposal of outdated digital devices.
-

9. **International Cooperation and Partnerships**

- Strengthening **collaboration with international organizations and IT companies** to adopt global best practices.
 - Facilitating **foreign investments in Nepal's ICT sector.**
-

10. **Legal and Regulatory Framework Development**

- Updating **ICT-related laws and policies** to align with global standards.
 - Establishing **strong regulatory bodies** to monitor digital transactions and ICT growth.
-

Conclusion

The **ICT Policy, 2072** focuses on **digitizing Nepal, enhancing cybersecurity, and promoting ICT-driven economic growth.** It aims to transform Nepal into a **knowledge-based economy** through technology and innovation.

7. What strategies are adopted in IT policy of Nepal to make information Technology accessible to the general public and increase employment through this means?

→ Strategies Adopted in the IT Policy of Nepal to Make IT Accessible and Increase Employment

Nepal's **IT Policy** focuses on making **Information Technology (IT)** accessible to the general public while increasing employment opportunities in the sector. Some key strategies include:

1. Expansion of ICT Infrastructure

- ✓ Development of **broadband internet and mobile connectivity** across urban and rural areas.
- ✓ Establishment of **community IT centers, telecenters, and free Wi-Fi zones** for public access.

2. Promotion of Digital Literacy and IT Education

- ✓ Inclusion of **IT as a compulsory subject** in schools and universities.
- ✓ Development of **technical training programs, coding boot camps, and IT skill development centers**.
- ✓ Encouragement of **online learning platforms and e-libraries** for digital education.

3. E-Governance and Digital Services

- ✓ Implementation of **e-governance to provide online public services**, making IT accessible to all.
- ✓ Development of **digital identity systems** (e.g., National ID, digital signatures) to ease access to government and financial services.

4. Development of IT Industry and Entrepreneurship

- ✓ Encouragement of **IT startups, innovation hubs, and incubators** for young entrepreneurs.
 - ✓ Establishment of **special economic zones (SEZs)** for IT parks and software industries.
 - ✓ Financial support and tax incentives for **IT companies, freelancers, and startups**.
-

5. Job Creation through IT Outsourcing and Freelancing

- ✓ Promotion of **Nepal as an IT outsourcing hub** for global companies.
 - ✓ Support for **freelancers through skill development, financial aid, and international market connections.**
 - ✓ Establishment of **co-working spaces and freelancing platforms** for IT professionals.
-

6. E-Commerce and Digital Payment Systems

- ✓ Encouragement of **online businesses and e-commerce platforms** to create digital job opportunities.
 - ✓ Promotion of **mobile banking, digital wallets, and online payment systems** to enhance financial inclusion.
-

7. Cybersecurity and Legal Framework Enhancement

- ✓ Strengthening **cyber laws to protect online businesses, digital transactions, and personal data.**
 - ✓ Establishing a **regulatory body to oversee IT development and digital safety.**
-

8. Public-Private Partnerships in IT Development

- ✓ Collaboration between the **government, private sector, and academic institutions** to boost IT innovation.
 - ✓ Attracting **foreign investment in Nepal's IT sector** to create more job opportunities.
-

Conclusion

The IT Policy of Nepal aims to **bridge the digital divide, create employment, and transform Nepal into a knowledge-based economy.** Through **digital literacy, infrastructure development, IT industry growth, and freelancing support,** Nepal is working towards **making IT accessible and employment-rich.**

8. What steps should be taken to reduce cyber crime? Explain with reference to IT policy implemented recently in Nepal.

→Steps to Reduce Cybercrime in Nepal (With Reference to the IT Policy of Nepal)

Cybercrime is a growing threat in Nepal, and the **IT Policy, 2072 (2015)** includes several measures to strengthen cybersecurity. Here are the key steps that should be taken to **reduce cybercrime** in Nepal:

1. **Strengthening Cyber Laws and Legal Framework**

- ✓ **Implementation of the Electronic Transaction Act (ETA), 2063**, which penalizes hacking, data breaches, and cyber fraud.
 - ✓ Establishment of **strict cyber laws** to regulate **social media misuse, identity theft, and financial fraud**.
 - ✓ Introduction of a **dedicated Cyber Crime Prevention Act** with **clear punishments** for digital offenses.
-

2. **Enhancing Cybersecurity Infrastructure**

- ✓ Development of **National Cyber Security Centers** to monitor and respond to cyber threats.
 - ✓ Strengthening **firewall systems, intrusion detection systems, and encryption standards** for national security.
 - ✓ Encouraging **secure web hosting** and **data centers in Nepal** to reduce dependency on foreign servers.
-

3. **Promoting Digital Literacy and Awareness**

- ✓ Conducting **cybersecurity awareness campaigns** at schools, colleges, and workplaces.
 - ✓ Educating **government employees, businesses, and individuals** about **safe online practices**.
 - ✓ Introducing **cyber ethics and responsible internet usage** in school curriculums.
-

4. **Strengthening Cyber Law Enforcement and Investigation**

- ✓ Establishment of a **dedicated Cyber Crime Investigation Bureau** within Nepal Police.
 - ✓ Training law enforcement officers in **digital forensics, cyber tracking, and hacking prevention**.
 - ✓ Collaborating with **Interpol, CERT (Computer Emergency Response Team), and IT experts** for cybercrime investigation.
-

5. Implementing Secure Digital Payment Systems

- ✓ Strengthening **fraud detection mechanisms** for e-banking, mobile banking, and e-wallets.
 - ✓ Encouraging **multi-factor authentication (MFA)** for online transactions.
 - ✓ Imposing **strict penalties for online financial fraud and phishing attacks**.
-

6. Regulating Social Media and Online Content

- ✓ Enforcing laws against **cyberbullying, harassment, fake news, and hate speech**.
 - ✓ Establishing a **national digital monitoring system** to track online criminal activities.
 - ✓ Promoting **responsible use of social media platforms**.
-

7. Encouraging Public-Private Partnerships in Cybersecurity

- ✓ Collaboration between the **government, IT industry, and academic institutions** to develop **cybersecurity research and innovation**.
 - ✓ Promoting **cybersecurity startups** that focus on **network security, ethical hacking, and malware detection**.
-

8. Strengthening International Cooperation in Cybersecurity

- ✓ Signing **cybersecurity agreements with global organizations** for cross-border cybercrime investigations.
 - ✓ Participating in **regional and global cybersecurity initiatives** to share threat intelligence.
-

Conclusion

The **IT Policy, 2072** of Nepal prioritizes **cybercrime prevention through legal reforms, infrastructure security, public awareness, and strong law enforcement**. Implementing these steps will **enhance digital security, protect user data, and make Nepal's cyberspace safer**.

9. Write about the role of controller (Digital certifying Authority) as mentioned in Electronic Transaction Act of Nepal.

→ **Role of the Controller (Digital Certifying Authority) as Mentioned in the Electronic Transaction Act of Nepal**

The **Electronic Transaction Act (ETA), 2063 (2008)** of Nepal establishes the role of the **Controller of Certification Authority (CCA)** to regulate digital certificates and ensure secure electronic transactions. The **Controller** is responsible for managing and overseeing **Certification Authorities (CAs)** that issue digital signatures.

Key Roles and Responsibilities of the Controller

1. Licensing and Regulation of Certification Authorities (CAs)

- Grants **licenses to Certification Authorities (CAs)** that issue digital certificates.
 - Monitors and regulates **CAs to ensure compliance with cybersecurity standards**.
 - Can **suspend or revoke licenses** of CAs that fail to comply with regulations.
-

2. Ensuring Security and Integrity of Digital Signatures

- Enforces **standards and guidelines** for issuing, using, and managing digital signatures.
 - Ensures that digital signatures and encryption techniques are **secure and reliable**.
 - Prevents the **misuse or forgery of digital certificates**.
-

3. Managing the National Digital Certification Framework

- Develops and maintains a **public key infrastructure (PKI)** to ensure **secure digital communications**.
 - Establishes **rules for cryptographic security** in electronic transactions.
 - Maintains a **repository of revoked and expired digital certificates**.
-

4. Handling Disputes and Investigations

- Investigates **complaints and fraud cases** related to digital certificates.
 - Resolves **disputes between users and Certification Authorities** regarding digital signatures.
 - Takes **legal action against entities involved in digital signature fraud**.
-

5. Promoting Public Awareness and Digital Security

- Conducts **awareness programs** to educate businesses, individuals, and government agencies on digital security.
 - Encourages the **adoption of digital certificates for secure transactions**.
 - Advises the **government on digital security policies and improvements**.
-

6. Collaboration with National and International Bodies

- Works with **law enforcement agencies** to combat cybercrimes.
 - Coordinates with **international cybersecurity organizations** to follow global best practices.
-

Conclusion

The **Controller of Certification Authority (CCA)** plays a vital role in **securing digital transactions, regulating Certification Authorities, and ensuring the reliability of digital signatures** in Nepal. This role is crucial in **enhancing trust in e-commerce, e-governance, and online services**.

10. What do you know about "The development of Nepal's IT policy". Also state what should be added or not added in IT policy 2067.

→The Development of Nepal's IT Policy

Nepal's **IT Policy**, also known as the **Information and Communication Technology (ICT) Policy**, has evolved over the years to adapt to the changing needs of the digital world. The first **National ICT Policy** was introduced in **2000**, and a revised version, **ICT Policy 2072 (2015)**, was developed to address contemporary challenges and opportunities in the IT sector.

The **development of Nepal's IT policy** is driven by several goals:

- **Digital Inclusion:** Ensuring access to technology and digital services for all Nepali citizens, especially in rural and underserved areas.
- **Economic Growth:** Leveraging ICT for boosting the national economy, generating employment, and creating a competitive IT sector.
- **E-Governance:** Promoting the use of digital technologies in government services for transparency, efficiency, and ease of access.
- **Cybersecurity:** Addressing the rise in cybercrime and establishing frameworks for securing online activities.

- **Human Resource Development:** Expanding the digital skills of the population to promote job creation, particularly in the IT sector.

The Current IT Policy (ICT Policy 2072)

Nepal's **ICT Policy 2072** focuses on:

- **Infrastructure Development:** Building widespread broadband connectivity and strengthening national digital infrastructure.
- **Digital Literacy:** Promoting IT education and training for the workforce.
- **Cybersecurity:** Enhancing national cybersecurity measures and creating legal frameworks for online security.
- **Promotion of IT Startups:** Creating incentives for new businesses in the IT sector.
- **Public-Private Partnerships:** Encouraging collaboration between the government and private sector to foster the growth of the IT industry.

What Should Be Added or Not Added in IT Policy 2067?

What Should Be Added

1. Data Privacy and Protection:

- The policy should explicitly address **data protection** and **privacy laws**. With increasing online transactions, there is a growing concern about the **protection of personal data**. The introduction of a **Data Protection Act** would safeguard citizens' rights.

2. Support for Digital Startups and Innovation:

- The policy should provide clear strategies and incentives to **promote IT startups**, especially in emerging technologies like **artificial intelligence, blockchain, and cloud computing**.
- Establishing **tech hubs** or **incubators** would support the growth of the IT ecosystem.

3. Cybersecurity Framework:

- With the increasing threats of cybercrime, the policy should adopt **comprehensive cybersecurity measures** such as the establishment of a **National Cybersecurity Center** and a **Cybersecurity Policy** to protect the digital infrastructure of the country.

4. Integration of Emerging Technologies:

- The policy should emphasize the adoption of **emerging technologies** like **IoT (Internet of Things)**, **5G networks**, **machine learning**, and **big data** for national development.
- 5. **Improved Internet Connectivity:**
 - Expanding high-speed **internet connectivity** to rural areas and ensuring **affordable internet access** for all citizens, as digital inclusion is vital for reducing the digital divide.
- 6. **Legal Reforms for E-commerce:**
 - The policy should focus on providing legal backing for **e-commerce** businesses, ensuring consumer rights and data protection for online shoppers, and making **online payment systems** secure.

What Should Not Be Added

1. **Excessive Bureaucratic Control:**
 - The policy should avoid too much **bureaucratic interference** in the growth of the IT sector. Overregulation could stifle innovation and reduce the efficiency of the private sector in driving digital transformation.
2. **Overly Restrictive Laws on Internet Freedom:**
 - There should be a balanced approach to **internet censorship**. The policy should not introduce measures that unduly limit **freedom of expression** or **online activism**, which could impact Nepal's open and democratic digital environment.
3. **Exclusion of Public-Private Partnerships (PPP):**
 - The policy should avoid excluding the **private sector** from contributing to the development of ICT infrastructure. Collaboration between **government agencies** and **private companies** is crucial for rapid technological growth.
4. **Limiting Outsourcing and Freelancing:**
 - Policies that limit the growth of **freelancing and IT outsourcing** should not be added. These sectors provide significant opportunities for **employment** and **foreign revenue** for Nepal's economy.

Conclusion

The development of Nepal's IT Policy has significantly contributed to the growth of the sector, but there is still room for improvement in areas like **data protection**, **emerging**

technology integration, and **cybersecurity**. Adding measures that promote **innovation**, **digital literacy**, and **inclusive growth** would be beneficial. However, the policy should avoid excessive regulation that could hinder growth and restrict opportunities in the sector.