

INFORMATION SECURITY AND CYBER LAW

8.1 DIGITAL SOCIETY AND COMPUTER ETHICS

Digital Society: a community in which computers, the internet, and digital devices have become a central part of everyday communication, work, education, and commerce, rather than an optional convenience.

Banking, government services, education, shopping, and even social relationships now run partly or entirely through digital channels. This shift brings real benefits (speed, convenience, wider access) but also creates new responsibilities and risks that didn't exist in a purely paper-based society, such as privacy, digital security, and appropriate online behavior.

Computer Ethics: the set of moral principles that guide how computers and digital technology should be used responsibly, covering both what's legal and what's simply the right thing to do.

- Respecting others' privacy and not accessing their data, accounts, or devices without permission
- Not using a computer to harm others, spread false information, or harass someone online
- Giving proper credit for others' work and not plagiarizing content
- Not using pirated software or violating copyright and licensing terms
- Using computer resources responsibly, without wasting shared resources such as network bandwidth

8.2 CONCEPT OF INFORMATION SECURITY

Information security is the practice of protecting digital data and systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

Information security is commonly explained using three core goals, often called the **CIA Triad**:



Principle	What It Means
Confidentiality	Only authorized people can access or view the data
Integrity	Data stays accurate and unaltered unless changed by an authorized person
Availability	Data and systems are accessible to authorized users whenever needed

A data breach at a bank, for instance, threatens confidentiality if account details are leaked, integrity if transaction records are tampered with, and availability if the breach forces the bank's servers offline.

8.3 CONCEPT OF CYBERCRIME

Cybercrime is any criminal activity that is carried out using a computer, network, or the internet, either as the target of the crime or as the tool used to commit it.

Type of Cybercrime	What It Involves
Hacking	Gaining unauthorized access to a computer system or network
Phishing	Tricking a user into revealing sensitive information (passwords, card details) through fake emails or websites
Identity Theft	Stealing someone's personal information to impersonate them, often for financial gain
Cyberbullying / Online Harassment	Using digital platforms to threaten, harass, or humiliate another person
Software Piracy	Illegally copying, distributing, or using licensed software without authorization
Financial Fraud	Unauthorized use of banking details, cards, or digital wallets for theft

8.4 MALICIOUS SOFTWARE AND SPAM

Malicious Software (Malware): any software specifically designed to damage, disrupt, or gain unauthorized access to a computer system, usually without the user's knowledge or consent.

Type	How It Behaves
Virus	Attaches itself to a legitimate file or program and spreads when that file is shared or run

Worm	Spreads on its own across a network, without needing to attach to another file
Trojan Horse	Disguises itself as legitimate software while carrying out harmful actions in the background
Spyware	Secretly monitors a user's activity and sends the collected data to a third party
Ransomware	Locks or encrypts a victim's files and demands payment to restore access
Adware	Automatically displays unwanted advertisements, often bundled with free software

Spam: unsolicited, often irrelevant or repetitive messages, typically sent in bulk over email or messaging platforms, usually for advertising or, in more harmful cases, to spread malware or phishing links.

8.5 PROTECTION FROM CYBERCRIME

Most protective measures come down to a handful of consistent habits:

- **Use strong, unique passwords** for different accounts, and change them periodically
- **Enable two-factor authentication (2FA)** wherever it's available, adding a second layer of verification beyond just a password
- **Keep software and operating systems updated**, since updates frequently patch known security vulnerabilities
- **Install and update antivirus software** to detect and remove known malware
- **Avoid clicking suspicious links or attachments**, especially in unexpected emails asking for personal or financial information
- **Use a firewall** to monitor and control incoming and outgoing network traffic
- **Back up important data regularly**, so it can be recovered even after an attack like ransomware
- **Be cautious about what personal information is shared** on social media and public platforms

8.6 INTELLECTUAL PROPERTY RIGHT

Intellectual Property Right (IPR) is the legal right that gives a creator control over the use of their own original creation, such as an invention, piece of writing, design, or software.

IPR exists so that creators can benefit from their own work and are protected against others copying or profiting from it without permission.

Type of IPR	What It Protects
Copyright	Original creative works, such as software, books, music, and films
Patent	New inventions or technical processes
Trademark	Brand names, logos, and symbols that identify a business or product
Trade Secret	Confidential business information, such as a formula or process, kept secret rather than publicly registered

Using pirated software or copying someone else's code, images, or written work without permission or credit is a direct violation of intellectual property rights, even if no money changes hands.

8.7 CONCEPT OF DIGITAL SIGNATURE

A digital signature is an electronic, cryptographic method used to verify the authenticity and integrity of a digital document or message, confirming who sent it and that it hasn't been altered since it was signed.

A digital signature is not simply a scanned image of a handwritten signature. It's generated mathematically using cryptography, tied to a unique digital certificate issued by a licensed certifying authority, which is what gives it legal recognition. In Nepal, this recognition and the certifying authority system are established under the Electronic Transaction Act 2063, covered in the next section.

- **Authentication:** confirms the identity of the sender
- **Integrity:** confirms the document hasn't been changed after signing
- **Non-repudiation:** prevents the signer from later denying that they signed the document

8.8 CONCEPT OF CYBER LAW IN NEPAL

Cyber law refers to the legal rules that govern activities carried out through computers, networks, and the internet, including electronic transactions, digital signatures, data protection, and cybercrime.

Nepal's primary cyber law is the **Electronic Transaction Act, 2063 (2006)**, commonly referred to as the ETA. It was Nepal's first law to formally recognize electronic activity, and it remains the country's foundational cyber legislation.

- **Legal recognition:** gives electronic records and digital signatures the same legal standing as paper documents and handwritten signatures
- **Certifying Authorities:** establishes a licensing and regulatory system (the Office of the Controller of Certification) for authorities that issue digital signature certificates

- **Cybercrime provisions:** defines offences such as unauthorized access (hacking), computer-related fraud, and the publication of illegal electronic material, along with penalties that can include fines and imprisonment
- **Dispute resolution:** establishes an Information Technology Tribunal to hear and resolve cases related to electronic transactions and cybercrime

One of its most cited provisions criminalizes publishing or displaying electronic material that is considered contrary to public morality or decent behaviour, or that spreads hate or discrimination — a section that has been used in a number of real cybercrime cases in Nepal and has also been the subject of public debate over how broadly it should be applied.

8.9 ICT POLICY IN NEPAL

An ICT Policy is a government framework that sets out the vision, goals, and strategies for developing and using information and communication technology across a country.

Nepal's current framework is the **ICT Policy, 2072 (2015)**, built around the vision of transforming Nepal into an information and knowledge-based society and economy.

- Expanding access to reliable, affordable internet and ICT infrastructure across the country, including rural areas
- Promoting e-governance, so government services can be delivered in a more transparent and efficient way
- Encouraging the growth of the IT industry as a contributor to Nepal's economy
- Improving digital literacy among the general population
- Supporting the use of ICT in education, healthcare, and other public sectors

Where the Electronic Transaction Act sets the legal rules for digital activity, the ICT Policy sets the broader national direction and goals for how technology should grow and be used across the country.