



KAMALDNP

kamaldnp.com • IT Training, Varanasi

PDF created by Raj Kamal using AI

Short Notes — Information Security

BTEUP Diploma in Computer Science & Engineering • 5th Semester • Short Notes
Session 2026-27

Short Revision Notes — prepared by KAMALDNP Academy from the official BTEUP 2026-27 syllabus. This is NOT a BTEUP board paper or publication.

These short notes cover **Information Security**, a programme elective in the BTEUP 2026-27 fifth-semester scheme for Computer Science and Engineering — students choose either this subject or Advance Computer Networks as one elective. In the 2026-27 scheme the subject is a **practicum**, so most marks come from practical work, but a clear theory base is still essential for the viva and for doing the practicals correctly.

Use the notes unit by unit: read the points, revise the one-line summary at the end, and try the likely question for each unit in your own words. Always match your final preparation with the official syllabus PDF and your lab records.

Unit 1 — Introduction to Information Security (8 Periods, 20%)

Topics: Introduction to information security; various aspects of information security (PAIN); security features of operating systems — authentication, logs, audit features, file system protection, user privileges, RAID options, anti-virus software, etc.

Introduction to information security and its aspects (PAIN)

Information security means protecting information and information systems from unauthorised access, use, disclosure, modification or destruction, so that data remains trustworthy throughout its life — in storage, in processing and in transit.

The syllabus summarises its aspects as **PAIN**:

- **Privacy (confidentiality)** — only authorised persons can read the information.
- **Authentication** — the identity of a user or system is verified before access is given.
- **Integrity** — information is not altered without detection; what is received is what was sent.
- **Non-repudiation** — a sender cannot later deny sending, and a receiver cannot deny receiving, a message.

Supporting ideas are availability (systems work when needed), access control, and accountability through records. Threats include malware, hackers, careless users and natural disasters; security combines technology, procedures and user awareness — the strongest password fails if the user shares it.

Security features of operating systems — authentication, logs, audit, file system protection, privileges, RAID and anti-virus

An operating system provides the first line of defence. Its main security features:

- **Authentication** — user IDs with passwords, and stronger methods where available, verify identity at login.
- **Logs** — the OS records logins, failures and important events; **audit features** let administrators review these records to trace suspicious activity.
- **File system protection** — permissions on files and folders decide who may read, write or execute them.
- **User privileges** — ordinary users get limited rights; administrator rights are separate, following the principle of least privilege.

RAID options (Redundant Array of Independent Disks) protect availability and data against disk failure by mirroring or striping data with parity across disks — RAID improves fault tolerance but is not a substitute for backup. **Anti-virus software** scans files and memory, blocks known malware by signatures and behaviour, and must be updated regularly to recognise new threats. Together these features protect the machine before any network security product is added.

Likely question: Explain the PAIN aspects of information security. Describe the security features available in an operating system.

Unit 2 — Security Weaknesses in Networks (10 Periods, 22%)

Topics: Understanding security weaknesses in popular networking protocols — IP, TCP, UDP, RIP, OSPF, HTTP, SMTP, etc.; security weaknesses in common networking devices — hub, switch, router, WiFi; security solutions to mitigate security risk of networking protocols (IPSec, HTTPS, etc.) and devices (VLAN, VPN, ingress filtering, etc.).

Security weaknesses in networking protocols — IP, TCP, UDP, RIP, OSPF, HTTP, SMTP

The popular networking protocols were designed for connectivity first, not security, so data often travels in plain form and identities are weakly checked.

- **IP** — no built-in authentication or encryption; source addresses can be spoofed and packets can be read in transit.
- **TCP** — connection setup can be abused (for example, flooding a server with half-open connections); sessions can be hijacked if sequence numbers are predicted.
- **UDP** — connectionless, with no delivery or identity checks; easy to spoof and abuse in flood attacks.
- **RIP and OSPF** — routing protocols can accept false route advertisements, diverting traffic, unless authentication is enabled.
- **HTTP** — web traffic in clear text; passwords and pages can be read or altered in transit.
- **SMTP** — mail transfer without strong sender verification, enabling spam and forged mail (spoofing/phishing).

The pattern to state in the exam: plain text, weak or no authentication, and trust in addresses that can be faked.

Security weaknesses in networking devices — hub, switch, router, WiFi

Common networking devices also have characteristic weaknesses:

- **Hub** — broadcasts every frame to all ports, so any connected machine can sniff all traffic; no intelligence, no control.
- **Switch** — better than a hub, but can be attacked by flooding its address table (forcing broadcast behaviour) or by abusing VLAN and spanning-tree features if unmanaged.
- **Router** — a prime target: weak or default passwords, outdated software and open management interfaces can give an attacker control of the whole network's traffic.
- **WiFi** — signals cross walls; weak encryption, default router passwords and rogue access points let outsiders join or imitate the network.

Device security therefore means changing defaults, updating firmware/software, disabling unused services and ports, and controlling who can administer the device. An unmanaged device should be treated as an untrusted device.

Security solutions — IPSec, HTTPS, VLAN, VPN and ingress filtering

Solutions are matched to the weaknesses of Unit 2's first two topics:

- **IPSec** — adds authentication and encryption at the IP layer, securing communication between hosts or networks regardless of the application.
- **HTTPS** — HTTP carried over TLS encryption, so web traffic, logins and payments cannot be read or silently altered in transit; the padlock also authenticates the website.

- **VLAN** — divides one physical LAN into separate logical networks, so a compromise or flood in one segment does not expose all departments.
- **VPN** — an encrypted tunnel over a public network gives remote users and branch offices private-network safety.
- **Ingress filtering** — routers drop incoming packets whose source addresses could not legitimately arrive from that direction, blocking spoofed traffic at the boundary.

Exam formula: encrypt what is plain (IPSec, HTTPS, VPN), segment what is flat (VLAN), and filter what is forged (ingress filtering).

Likely question: Discuss the security weaknesses of any three networking protocols. How do IPSec, HTTPS, VLAN and VPN reduce network risk?

Unit 3 — Cryptography and Secure Development (8 Periods, 20%)

Topics: Basics of cryptography; PKI; security considerations while developing software.

Basics of cryptography

Cryptography is the science of protecting information by transforming it into an unreadable form that only authorised persons can reverse. Basic terms: **plaintext** (original message), **ciphertext** (scrambled result), **encryption** (plaintext to ciphertext), **decryption** (reverse process) and the **key** (secret value controlling the transformation).

- **Symmetric cryptography** — the same key encrypts and decrypts. Fast and suitable for bulk data, but the key must be shared secretly in advance.
- **Asymmetric cryptography** — a mathematically linked **public key** (shared openly, encrypts) and **private key** (kept secret, decrypts). Solves key distribution and enables digital signatures.
- **Hashing** — a one-way function producing a fixed-length fingerprint of data; any change in data changes the fingerprint, so hashing protects integrity and stores password verifiers.

In practice the two key systems combine: asymmetric methods exchange a fresh symmetric key, and symmetric encryption carries the actual data quickly.

PKI — Public Key Infrastructure

PKI (Public Key Infrastructure) is the complete system that makes public-key cryptography trustworthy in practice. Its problem: a public key is useful only if you are sure whose key it really is.

Main components:

- **Digital certificate** — an electronic document binding a public key to an identity, digitally signed by an authority.

- **Certificate Authority (CA)** — the trusted body that verifies identity and issues certificates.
- **Registration Authority (RA)** — checks applicants' identity details before the CA issues.
- **Certificate repository and revocation list** — where certificates are published, and how cancelled certificates (for example, after a key leak) are announced.

Everyday example: HTTPS websites present certificates issued through PKI, and the browser verifies the CA's signature before trusting the site. Without PKI, an attacker could publish a fake key in a victim's name and defeat asymmetric encryption completely.

Security considerations while developing software

Most breaches exploit badly written software, so security must be built in **while developing**, not patched afterwards. Core considerations:

- **Validate all input** — never trust data from users or other systems; unchecked input enables injection and overflow attacks.
- **Protect secrets** — never hard-code passwords or keys in code; store password verifiers as salted hashes, not plain text.
- **Least privilege** — the software and its database account should have only the rights they truly need.
- **Handle errors safely** — show users simple messages; detailed technical errors help attackers map the system.
- **Keep components updated** and test security before release, including review by someone other than the author.

Also plan for logging of security events and a safe update mechanism. One-line summary for viva: secure development = validate input, protect secrets, give minimum rights, and test before release.

Likely question: Describe briefly the basics of cryptography. What is PKI and what are its main components?

Unit 4 — Network Security Products (8 Periods, 20%)

Topics: Network security products — firewall, IDS/IPS, VPN concentrator, content screening gateways, etc.

Firewall and IDS/IPS

A **firewall** is a barrier between a trusted internal network and an untrusted network (usually the internet). It examines passing traffic against a rule set — based on addresses, ports, protocols and connection state — and allows or blocks it. Firewalls may be software on a host or a dedicated hardware appliance at the network boundary. A correctly written rule set follows the principle: deny by default, allow only what is needed.

An **IDS (Intrusion Detection System)** monitors traffic or host activity for signs of attack and raises an alert — it detects but does not block. An **IPS (Intrusion Prevention System)** sits in the traffic path and can actively drop malicious packets and block the attacker, preventing the intrusion, not only reporting it.

Difference in one line: a firewall filters by rules on known traffic types, an IDS watches and warns, and an IPS watches and acts. All three need updated signatures/rules and someone who actually reads the alerts.

VPN concentrator and content screening gateways

A **VPN concentrator** is a dedicated device that handles many VPN connections at one point — typically at the head office where remote users and branch offices connect. It performs the heavy work of tunnel setup, authentication and encryption/decryption for large numbers of simultaneous sessions, so individual servers are not burdened. It centralises VPN policy: who may connect, with what authentication, and to which internal resources.

A **content screening gateway** inspects the content of traffic rather than only its addresses — it scans web pages and downloads for malware, filters objectionable or unapproved websites, and can block leakage of sensitive data in outgoing mail or uploads. Placed at the internet gateway, it protects users from harmful content and protects the organisation from policy violations.

'Etc.' in the syllabus points to similar boundary products — anti-spam gateways, web proxies and unified threat management (UTM) boxes that combine several of these functions in one appliance.

Likely question: Differentiate between IDS and IPS. Describe the role of a firewall and a VPN concentrator in network security.

Unit 5 — Security Standards, Audit and Policy (8 Periods, 18%)

Topics: Introduction to security standards — ISO 27001, Indian IT Act, IPR laws; security audit procedures; developing security policies; disaster recovery; business continuity planning.

Security standards — ISO 27001, Indian IT Act and IPR laws

ISO 27001 is the international standard for an **Information Security Management System (ISMS)** — a systematic way for an organisation to identify its information risks, apply suitable controls, and keep improving them. Certification shows customers and partners that security is managed, not accidental.

The **Indian IT Act** (Information Technology Act, 2000, as amended) is India's main cyber law. It gives legal recognition to electronic records and digital signatures, and defines offences and

penalties for acts such as unauthorised access, data theft and computer-related fraud — students should know it as the legal backbone of Indian information security.

IPR laws (Intellectual Property Rights) — copyright, patents, trademarks — protect software and digital content legally; using pirated software is both a legal violation and a security risk, since pirated copies often carry malware. Standards tell an organisation what good practice is; the law sets what is punishable — both shape security decisions.

Security audit procedures and developing security policies

A **security audit** is a systematic, independent examination of whether an organisation's security controls exist, work as intended, and match its policy and standards. Typical procedure:

- Define scope and collect documents — policies, network diagrams, access lists.
- Inspect configurations, interview staff, and test controls (for example, checking for default passwords or outdated systems).
- Record findings with severity, recommend corrective actions with priorities, and re-check after fixes.

A **security policy** is the organisation's written rulebook that the audit tests against. Developing it involves identifying assets and risks, deciding rules for passwords, access, internet and email use, data backup and incident reporting, getting management approval, informing all staff, and reviewing it regularly. A policy nobody knows exists protects nothing — awareness is part of the control.

Disaster recovery and business continuity planning

Disaster recovery (DR) is the plan for restoring IT systems and data after a major incident — fire, flood, ransomware or total server failure. It specifies backups and where they are kept, recovery priorities, the order in which systems are rebuilt, and the team responsible. Two classic measures are how much data loss is acceptable (recovery point) and how fast service must return (recovery time).

Business continuity planning (BCP) is wider: it plans how the organisation's essential work continues during and after a disruption — alternate workplace, manual workarounds, communication with customers and suppliers — not only how computers are restored.

Relationship in one line: disaster recovery is a part of business continuity; DR restores the IT, BCP keeps the business running. Both plans must be documented, assigned to named people, and tested with practice drills — an untested plan usually fails on the day it is needed.

Likely question: Write a short note on ISO 27001 and the Indian IT Act. Differentiate between disaster recovery and business continuity planning.

Quick Revision — One Line Each

- PAIN = Privacy, Authentication, Integrity, Non-repudiation — the four aspects of information security.
- Authentication proves who you are; authorisation decides what you are allowed to do.
- Logs and audit trails record who did what and when — they support detection and accountability.
- Plain IP, TCP, UDP, HTTP and SMTP were not designed with strong security built in.
- IPSec secures IP communication; HTTPS is HTTP over TLS for secure web traffic.
- VLAN segments a LAN; VPN creates an encrypted tunnel over a public network.
- Symmetric cryptography uses one shared key; asymmetric (PKI) uses a public-private key pair; a CA issues certificates.
- Firewall filters traffic by rules; IDS only alerts, IPS can also block the attack.
- ISO 27001 is the standard for an information security management system (ISMS).
- Indian IT Act gives legal recognition to electronic records and covers computer offences.
- Security audit = systematic checking against policy and standards; findings drive corrective action.
- Disaster recovery restores IT after a disaster; business continuity keeps essential work running through it.

KAMALDNP • kamaldnp.com • support@kamaldnp.com • +91 8318013442 • Varanasi, UP

Prepared by KAMALDNP Academy from the official BTEUP 2026-27 syllabus topics. Short explanations are the author's own plain-English summaries, not syllabus text. Please confirm with your own polytechnic for any local changes.