Information Security vs Cybersecurity

Information security differs from cybersecurity in both scope and purpose. The two terms are often used interchangeably, but more accurately, cybersecurity is a subcategory of information security. Information security is a broad field that covers many areas such as physical security, endpoint security, data encryption, and network security. It is also closely related to information assurance, which protects information from threats such as natural disasters and server failures.

Cybersecurity primarily addresses technology-related threats, with practices and tools that can prevent or mitigate them. Another related category is data security, which focuses on protecting an organization's data from accidental or malicious exposure to unauthorized parties.

Information Security Threats

Unsecure or Poorly Secured Systems

The speed and technological development often leads to compromises in security measures. In other cases, systems are developed without security in mind, and remain in operation at an organization as legacy systems. Organizations must identify these poorly secured systems, and mitigate the threat by securing or patching them, decommissioning them, or isolating them.

Social Media Attacks

Many people have social media accounts, where they often unintentionally share a lot of information about themselves. Attackers can launch attacks directly via social media, for example by spreading malware via social media messages, or indirectly, by using information obtained from these sites to analyze user and organizational vulnerabilities, and use them to design an attack.

Social Engineering

Social engineering involves attackers sending emails and messages that trick users into performing actions that may compromise their security or divulge private information. Attackers manipulate users using psychological triggers like curiosity, urgency or fear.

Because the source of a social engineering message appears to be trusted, people are more likely to comply, for example by clicking a link that installs malware on their device, or by providing personal information, credentials, or financial details.

Organizations can mitigate social engineering by making users aware of its dangers and training them to identify and avoid suspected social engineering messages. In addition, technological systems can

be used to block social engineering at its source, or prevent users from performing dangerous actions such as clicking on unknown links or downloading unknown attachments.

Malware on Endpoints

Organizational users work with a large variety of endpoint devices, including desktop computers, laptops, tablets, and mobile phones, many of which are privately owned and not under the organization's control, and all of which connect regularly to the Internet.

A primary threat on all these endpoints is malware, which can be transmitted by a variety of means, can result in compromise of the endpoint itself, and can also lead to privilege escalation to other organizational systems.

Traditional antivirus software is insufficient to block all modern forms of malware, and more advanced approaches are developing to securing endpoints, such as endpoint detection and response (EDR).

Lack of Encryption

Encryption processes encode data so that it can only be decoded by users with secret keys. It is very effective in preventing data loss or corruption in case of equipment loss or theft, or in case organizational systems are compromised by attackers.

Unfortunately, this measure is often overlooked due to its complexity and lack of legal obligations associated with proper implementation. Organizations are increasingly adopting encryption, by purchasing storage devices or using cloud services that support encryption, or using dedicated security tools.

Security Misconfiguration

Modern organizations use a huge number of technological platforms and tools, in particular web applications, databases, and Software as a Service (SaaS) applications, or Infrastructure as a Service (IaaS) from providers like Amazon Web Services.

Enterprise grade platforms and cloud services have security features, but these must be configured by the organization. Security misconfiguration due to negligence or human error can result in a security breach. Another problem is "configuration drift", where correct security configuration can quickly become out of date and make a system vulnerable, unbeknownst to IT or security staff.

Organizations can mitigate security misconfiguration using technological platforms that continuously monitor systems, identify configuration gaps, and alert or even automatically remediate configuration issues that make systems vulnerable.

How important is an information security policy?

Increased digitization leads to every user on a network generating, storing and sharing data, and there is always a part of that data that needs to be protected from unauthorized access. Whether it's for legal, internal or ethical concerns, sensitive data, PII and intellectual property must be protected in order to avoid catastrophic security incidents such as a data breach.

An information security policy details how the data is protected and evaluates all gaps that can be exploited by cybercriminals to access that data, as well as processes that are used to mitigate and recover from security incidents. This means it plays a crucial role in risk management and furthermore addresses an organization's needs and ways to comply with increasingly stringent regulatory compliance requirements.

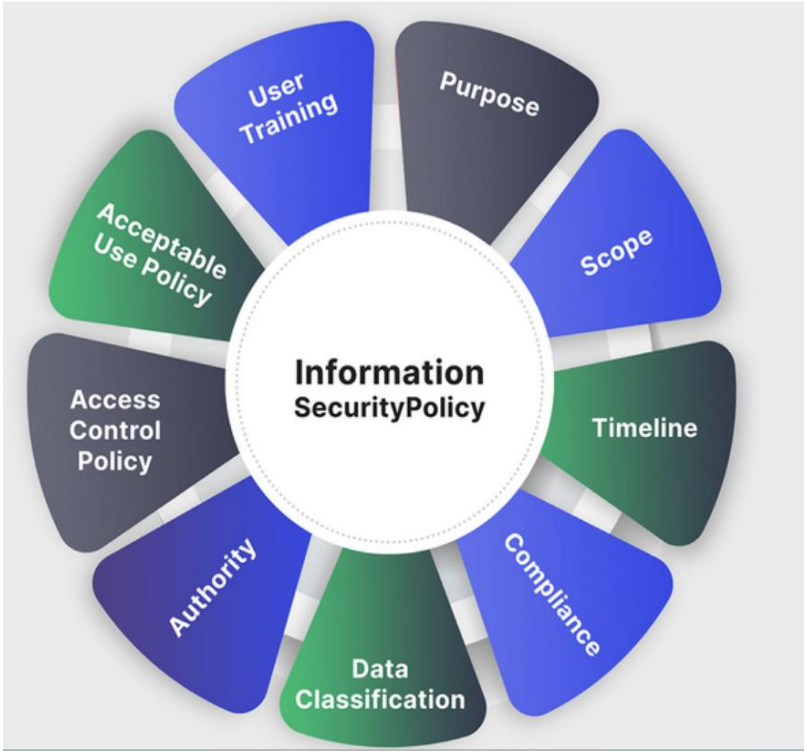
The importance of an information security policy

Information security policies can have the following benefits for an organization:

- **Facilitates data integrity, availability, and confidentiality** —ffective information security policies standardize rules and processes that protect against vectors threatening data integrity, availability, and confidentiality.
- **Protects sensitive data — I**nformation security policies prioritize the protection of intellectual property and sensitive data such as personally identifiable information (PII).
- **Minimizes the risk of security incidents — A**n information security policy helps organizations define procedures for identifying and mitigating vulnerabilities and risks. It also details quick responses to minimize damage during a security incident.
- **Executes security programs across the organization — I**nformation security policies provide the framework for operationalizing procedures.
- **Provides a clear security statement to third parties** — Information security policies summarize the organization’s security posture and explain how the organization protects IT resources and assets. They facilitate quick response to third-party requests for information by customers, partners, and auditors.

- **Helps comply with regulatory requirements** — Creating an information security policy can help organizations identify security gaps related to regulatory requirements and address them.

Information security policy key elements



Purpose

The first, and therefore most crucial, element of an information security policy is a clearly defined purpose. While the overarching goal of any security policy is to protect an organization's critical digital information, a more concrete and actionable purpose enables organizations to tailor security measures and guidelines, provide protection of their data, and reach their objectives.

Some of the more common purposes for organizations implementing an information security policy are:

- To enforce a security program and approach to information security across the organization
- To comply with legal, regulatory and industry requirements
- To keep brand reputation with regards to data security
- To detect and respond to data breaches and other security incidents

Scope

Modern organizations are large and can have a lot of dependencies, including third and fourth party vendors, technology users, and more. And as with every document, an information security policy should clearly mention the scope of the audience to whom the policy applies. It is generally recommended that the audience scope remains inclusive over data shared with third parties even if not legally obligated to do so, as many organizations omit them from their policies. Leaving it outside of the set rules and guidelines of an organization's policy can open that data up to compromise, without proper controls.

Another important aspect of scope is the governed infrastructure in the policy, which will ideally include all assets: all data, systems, programs, apps, etc. This allows, again, for a better overview and the protection of all parts of an infrastructure, empowering organizations to reduce their attack surface and consequently security risks.

Timeline

Particularly important for information security policies with the purpose of complying with regulatory requirements, a timeline is simply an element of the ISP that dictates the effective date of the policy.

Compliance

Another key ISP element that's designed to help an organization achieve and maintain regulatory compliance, the document should list all regulations that the policy is intended to help the organization comply with (with common ones including PCI DSS, HIPAA, and SOX), and how the organization achieves compliances with them.

Data classification

All data and assets that were pre-defined in the scope of the security policy are not equal, and are of different value to the organization. Classifying data based on its value will then inform specific handling procedures for each class. This can help organizations protect the data that actually matters, without needlessly expending resources to protect insignificant information. Data is usually classified based on the risk it can pose to the organization if compromised, so we have high risk data that is generally highly sensitive, private and covered by government regulations; confidential data that is not protected by the law but holds significance to the organization; and public data, which is publicly accessible and doesn't represent risk being so.

Authority

"Authority" refers to who has the authority to decide which data can be shared, and with whom. Typically, it follows a hierarchical pattern where the higher the position one holds in an organization, the more authority one has to make decisions about data and its share. For example, higher-level managers and executives have more insights into an organization's overall posture and operation, so they have the right to grant access to information as they see fit.

Simultaneously, a junior employee may be tied to sharing very little information they have access to, as they don't have the same level of insight and authority to grant access to it to others. An IT security policy should have terms that address every level of authority through all of the organization's seniorities and their data authorization, all of which should be a part of the access control policy.

Access control policy

Once the authority hierarchy has been decided on, it should be included in the access control policy. An access control policy helps document the amount of authority each level throughout an organization has over its data and assets, as well as how sensitive data is handled, access controls that are utilized and the minimum security standards for data access the organization must meet.

While an access control policy is dependent on an organization's security and business needs, common components include:

- The need-to-know principle, or principle of least privilege, which states that the user should be given permission to access only those resources needed to perform their job, reducing exposure of sensitive information
- A password policy that dictates the rules around password security such as the complexity of passwords, the timeline in which they need to be changed and how they're handled
- Physical access rules that apply to data storage centers, server rooms, and other physical locations and resources
- Instructions on how to remove users' access and their ability to interact with the organization's resources—critical now that we live in a time of widely accepted remote work policies

Acceptable usage policy

Organizations commonly maintain a list of resources that are restricted to their users. Whether its instructions on where users can find programs and apps to download when needed or using proxies to block viewing of social media and other websites for sharing information from an organization's network, it's important for organizations to document what is not required or even restricted from accessing to their users.

User training and behaviour

While an information security policy commonly has an objective of complying with regulatory requirements, or having a clear way to communicate guidelines to third parties, it does contain a set of rules that need to be enforced in an organization and followed by users.

Those users can't simply receive a document that showcases their expected behavior—security awareness and other user training should follow. Implementing security training and maintaining cybersecurity culture in an organization ensures that all users understand what is asked from them and what role they play in an organization's security program, and offers support as users are the most crucial components of a properly functioning ISP.

Other critical components of an information security policy

Here are just a few of other components that are generally included in a mature information security policy:

- **Change management policy** outlines formal processes and procedures for responding to changes that can affect the CIA of information.
- **Incident response policy** outlines how an organization responds to and mitigates security incidents, as well as their incident response process.
- **Information retention** refers to how data is stored and backed up as well as a retention schedule for when the information should be maintained.
- **Disaster recovery policy** is crucial in ensuring business continuity in the event of a potentially disruptive incident, whether it's a security breach or a natural disaster.
- **Identity and access management policy** outlines types of devices in use for systems and apps, standard for creating and authorizing accounts and how accounts are deprovisioned.
- **Personal device policy** goes hand in hand with remote access policies, as with high number of remote users comes a larger volume of personal devices being used to access organization's premises. This policy dictates which devices are allowed to access which information and systems, as well as authentication methods to do so.
- **Patch management** applies the specific procedures for patching and updating operating systems, software, antivirus solutions, etc.

Best practices for successful information security policies

1. **Information and data classification** — helps an organization understand the value of its data, determine whether the data is at risk, and implement controls to mitigate risks
2. **Developers, security, and IT operations** — should work together to meet compliance and security requirements. Lack of cooperation between departments may lead to configuration errors. Teams that work together in a DevSecOps model can coordinate risk assessment and identification throughout the software development lifecycle to reduce risks.
3. **Security incident response plan** — helps initiate appropriate remediation actions during security incidents. A security incident strategy provides a guideline, which includes initial threat response, priorities identification, and appropriate fixes.
4. **SaaS and cloud policy** — provides the organization with clear cloud and SaaS adoption guidelines, which can provide the foundation for a unified cloud ecosystem and standards of configuration, especially for development environments. This policy can help mitigate ineffective complications and poor use of cloud resources.
5. **Acceptable use policies (AUPs)** — helps prevent data breaches that occur through misuse of company resources. Transparent AUPs help keep all personnel in line with the proper use of company technology resources.

6. **Identity and access management (IAM) regulations** — let IT administrators authorize systems and applications to the right individuals and let employees know how to use and create passwords in a secure way. A simple password policy can reduce identity and access risks.
7. **Data security policy** — outlines the technical operations of the organization and acceptable use standards in accordance with all applicable governance and compliance regulations.
8. **Privacy regulations** — government-enforced regulations such as GDPR and CCPA protect the privacy of end users. Organizations that don't protect the privacy of their users risk fines and penalties, and in some cases court action.
9. **Personal and mobile devices** — Nowadays, most organizations have moved business processes to the cloud. Companies that permit employees to access company software assets from any location from any device risk introducing vulnerabilities through personal devices such as laptops and smartphones. Creating a policy for proper security of personal devices can help prevent exposure to threats via employee-owned assets.

Policy

Policies are formal statements produced and supported by senior management.

They can be organization-wide, issue-specific, or system-specific. Your organization's policies should reflect your objectives for your information security program—protecting information, risk management, and infrastructure security. Your policies should be like a building foundation; built to last and resistant to change or erosion.

- Driven by business objectives and convey the amount of risk senior management is willing to accept.
- Easily accessible and understood by the intended reader
- Created with the intent to be in place for several years and regularly reviewed with approved changes made as needed.

Standard

Standards are mandatory courses of action or rules that give formal policies support and direction.
One of the more difficult parts of writing standards for an information security program is getting a company-wide consensus on what standards need to be in place. This can be a time-consuming process but is vital to the success of your information security program.

- Used to indicate expected user behaviour. For example, a consistent company email signature.
- Might specify what hardware and software solutions are available and supported.
- Compulsory and must be enforced to be effective (this also applies to policies).

Procedure

Procedures are detailed step-by-step instructions to achieve a given goal or mandate.

They are typically intended for internal departments and should adhere to strict change control processes. Procedures can be developed as you go. If this is the route your organization chooses to take it's necessary to have comprehensive and consistent documentation of the procedures that you are developing.

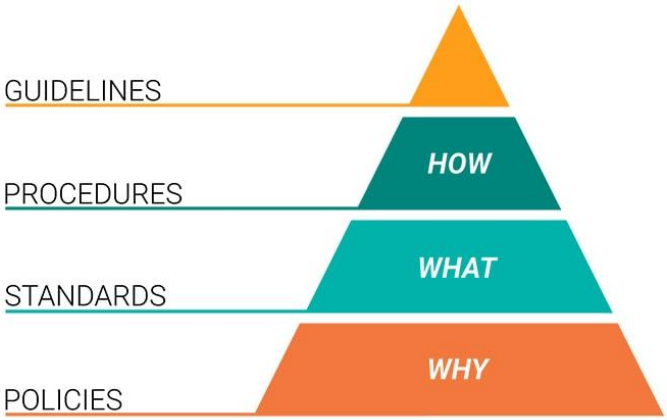
- Often act as the "cookbook" for staff to consult to accomplish a repeatable process.
- Detailed enough and yet not too difficult that only a small group (or a single person) will understand.
- Installing operating systems, performing a system backup, granting access rights to a system, and setting up new user accounts are all examples of procedures.

Guideline

Guidelines are recommendations to users when specific standards do not apply.

Guidelines are designed to streamline certain processes according to what the best practices are. Guidelines, by nature, should open to interpretation and do not need to be followed to the letter.

- Are more general vs. specific rules.
- Provide flexibility for unforeseen circumstances.
- Should NOT be confused with formal policy statements.

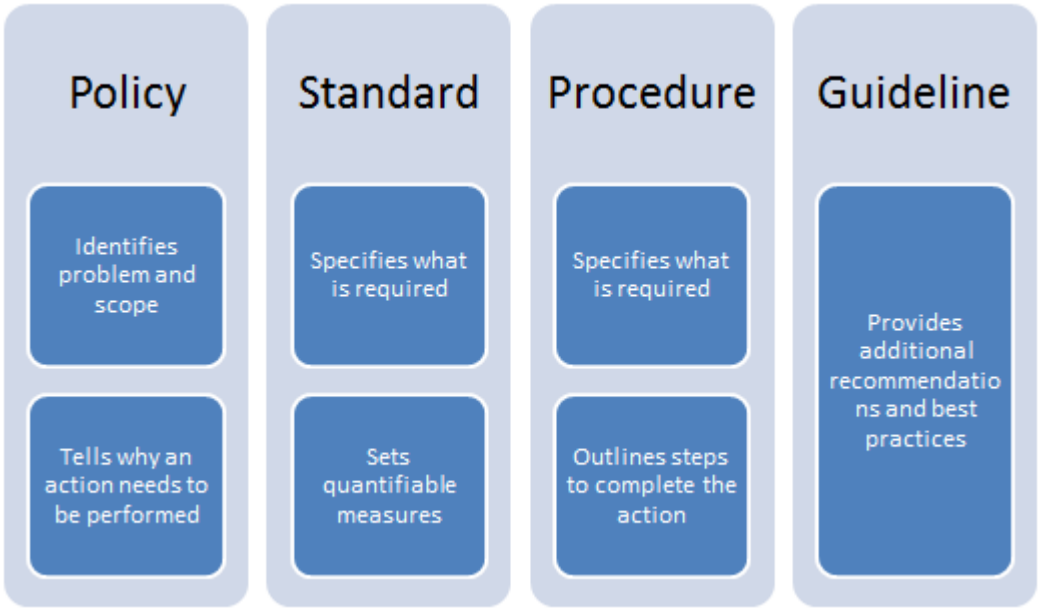


What are the Best Practices for Information Security Management?

A mature information security policy will outline or refer to the following policies:

1. **Acceptable use policy (AUP):** Outlines the constraints an employee must agree to use a corporate computer and/or network
2. **Access control policy (ACP):** Outlines access controls to an organization's data and information systems
3. **Change management policy:** Refers to the formal process for making changes to IT, software development and security
4. **Information security policy:** High-level policy that covers a large number of security controls
5. **Incident response (IR) policy:** An organized approach to how the organization will manage and remediate an incident

6. **Remote access policy:** Outlines acceptable methods of remotely connecting to internal networks
7. **Email/communication policy:** Outlines how employees can use the business's chosen electronic communication channel such as email, slack or social media
8. **Disaster recovery policy:** Outlines the organization's cybersecurity and IT teams input into an overall business continuity plan
9. **Business continuity plan (BCP):** Coordinates efforts across the organization and is used in the event of a disaster to restore the business to a working order
10. **Data classification policy:** Outlines how your organization classifies its data
11. **IT operations and administration policy:** Outlines how all departments and IT work together to meet compliance and security requirements.
12. **SaaS and cloud policy:** Provides the organization with clear cloud and SaaS adoption guidelines, this helps mitigate third-party and fourth-party risk
13. **Identity access and management (IAM) policy:** Outlines how IT administrators authorize systems and applications to the right employees and how employees create passwords to comply with security standards
14. **Data security policy:** Outlines the technical requirements and acceptable minimum standards for data security to comply with relevant laws and regulations
15. **Privacy regulations:** Outlines how the organization complies with government-enforced regulations such as GDPR that are designed to protect customer privacy
16. **Personal and mobile devices policy:** Outlines if employees are allowed to use personal devices to access company infrastructure and how to reduce the risk of exposure from employee-owned assets.



Information Technology Act, 2000 (India):

The **Information Technology Act, 2000** (also known as **ITA-2000**, or the **IT Act**) is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000. It is the primary law in India dealing with cybercrime and electronic commerce.

The Information Technology Act, 2000 also Known as an **IT Act** is an act proposed by the Indian Parliament reported on 17th October 2000. This Information Technology Act is based on the United Nations Model law on Electronic Commerce 1996 (UNCITRAL Model) which was suggested by the General Assembly of United Nations by a resolution dated on 30th January, 1997. It is the most important law in India dealing with Cybercrime and E-Commerce.
The main objective of this act is to carry lawful and trustworthy electronic, digital and online transactions and alleviate or reduce cybercrimes. The IT Act has 13 chapters and 90 sections. The last four sections that starts from 'section 91 – section 94', deals with the revisions to the Indian Penal Code 1860.

1. Tampering with the computer source documents.
2. Directions of Controller to a subscriber to extend facilities to decrypt information.
3. Publishing of information which is obscene in electronic form.
4. Penalty for breach of confidentiality and privacy.
5. Hacking for malicious purposes.
6. Penalty for publishing Digital Signature Certificate false in certain particulars.
7. Penalty for misrepresentation.
8. Confiscation.
9. Power to investigate offences.
10. Protected System.
11. Penalties for confiscation not to interfere with other punishments.
12. Act to apply for offence or contravention committed outside India.
13. Publication for fraud purposes.
14. Power of Controller to give directions.

Sections and Punishments under Information Technology Act, 2000 are as follows:

SECTION	PUNISHMENT
Section 43	**This section of IT Act, 2000 states that any act of destroying, altering or stealing computer system/network or deleting data with malicious intentions without authorization from owner of the computer is liable for the payment to be made to owner as compensation for damages.**
Section 43A	**This section of IT Act, 2000 states that any corporate body dealing with sensitive information that fails to implement reasonable security practices causing loss of other person will also liable as convict for compensation to the affected party.**

Section 66	**Hacking of a Computer System with malicious intentions like fraud will be punished with 3 years imprisonment or the fine of Rs.5,00,000 or both.**
Section 66 B, C, D	**Fraud or dishonesty using or transmitting information or identity theft is punishable with 3 years imprisonment or Rs. 1,00,000 fine or both.**
Section 66 E	**This Section is for Violation of privacy by transmitting image of private area is punishable with 3 years imprisonment or 2,00,000 fine or both.**
Section 66 F	**This Section is on Cyber Terrorism affecting unity, integrity, security, sovereignty of India through digital medium is liable for life imprisonment.**
Section 67	**This section states publishing obscene information or pornography or transmission of obscene content in public is liable for imprisonment up to 5 years or fine of Rs. 10,00,000 or both.**

What is the Information Technology Amendment Act 2008 (IT Act 2008)?
Tuesday, October 27, 2009, Press Information Bureau , Government of India

The Information Technology (Amendment) Act, 2008 has come into force today. The Rules pertaining to section 52 (Salary, Allowances and Other Terms and Conditions of Service of Chairperson and Members), section 54 (Procedure for Investigation of Misbehavior or Incapacity of Chairperson and Members), section 69 (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) , section 69A (Procedure and Safeguards for Blocking for Access of Information by Public), section 69B (Procedure and safeguard for Monitoring and Collecting Traffic Data or Information) and notification under section 70B for appointment of the Indian Computer Emergency Response Team have also been notified.

The Information Technology Act was enacted in the year 2000 with a view to give a fillip to the growth of electronic based transactions, to provide legal recognition for e-commerce and e-transactions, to facilitate e-governance, to prevent computer based crimes and ensure security practices and procedures in the context of widest possible use of information technology worldwide.

With proliferation of information technology enabled services such as e-governance, e-commerce and e-transactions; data security, data privacy and implementation of security practices and procedures relating to these applications of electronic communications have assumed greater importance and they required harmonization with the provisions of the Information Technology Act. Further, protection of Critical Information Infrastructure is pivotal to national security, economy, public health and safety, thus it had become necessary to declare such infrastructure as protected system, so as to restrict unauthorised access.

Further, a rapid increase in the use of computer and Internet has given rise to new forms of crimes like, sending offensive emails and multimedia messages, child pornography, cyber terrorism, publishing sexually explicit materials in electronic form, video voyeurism, breach of confidentiality and leakage of data by intermediary, e-commerce frauds like cheating by personation - commonly known as phishing, identity theft, frauds on online auction sites, etc. So, penal provisions were required to be included in the Information Technology Act, 2000. Also, the Act needed to be

technology-neutral to provide for alternative technology of electronic signature for bringing harmonization with Model Law on Electronic Signatures adopted by United Nations Commission on International Trade Law (UNCITRAL).

Keeping in view the above, Government had introduced the Information Technology (Amendment) Bill, 2006 in the Lok Sabha on 15th December 2006. Both Houses of Parliament passed the Bill on 23rd December 2008. Subsequently the Information Technology (Amendment) Act, 2008 received the assent of President on 5th February 2009 and was notified in the Gazette of India.

- **Section 69A and the Blocking Rules: Allowing the Government to block content under certain circumstances**

  Section 69A of the IT (Amendment) Act, 2008, allows the Central Government to block content where it believes that this content threatens the security of the State; the sovereignty, integrity or defence of India; friendly relations with foreign States; public order; or to prevent incitement for the commission of a cognisable offence relating to any of the above. A set of procedures and safeguards to which the Government has to adhere when doing so have been laid down in what have become known as the Blocking Rules.

- **Section 79 and the IT Rules: Privatising censorship in India**

  Section 79 of the Information Technology (Amendment) Act, 2008 regulates the liability of a wide range of intermediaries in India. The section came in the limelight mostly because of the infamous Intermediary Guidelines Rules, or IT Rules, which were made under it. The IT Rules constitute an important and worrying move towards the privatisation of censorship in India.

- **Sections 67 and 67A: No nudity, please**

  The large amounts of ‘obscene’ material that circulate on the Internet have long attracted comment in India. Not surprisingly, then, in the same way as obscenity is prohibited offline in the country, so it is online as well. The most important tools to curtail it are sections 67 and 67A of the IT Act, prohibiting obscene and sexually explicit material respectively.

- **Section 66A: Do not send offensive messages**

  Section 66A of the Information Technology (Amendment) Act, 2008 prohibits the sending of offensive messages though a communication device (i.e. through an online medium). The types of information this covers are offensive messages of a menacing character, or a message that the sender knows to be false but is sent for the purpose of ‘causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will.’ If you’re booked under Section 66A, you could face up to 3 years of imprisonment along with a fine.

People, Process and Technology:

People, Process, and Technology (PPT) is an approach to getting things done in which these three factors are all considered and balanced. Employees complete organizational tasks with the help of established procedures and, frequently, technological tools.