1. Objective of the Policy:

The objective of the Information/cyber/Cyber Security Policy is to provide, an approach to managing information/cyber risks and directives for the protection of information/cyber assets to, and those contracted to provide services.

2. Scope of the Policy:

This policy applies to all employees, contractors, partners, Interns/Trainees working in Unitech Plasto Components. Third party service providers providing hosting services or wherein data is held outside Unitech Plasto Components premises, shall also comply with this policy.

3. Frame Work:

3.1 Information/Cyber Security Governance:

Information/cyber security governance consists of leadership, organisational structures and processes that protect information and mitigation of growing information/cyber security threats Critical outcomes of information/cyber security governance include:

1. Alignment of information/cyber security with business strategy to support organisational objectives.

2. Management and mitigation of risks and reduction of potential impacts on information resources to an acceptable level.

3. Management of performance of information/cyber security by measuring, monitoring and reporting information security governance metrics to ensure that organisational objectives are achieved.

4. Optimisation of information security investments in support of organisational Objectives.

It is important to consider the organisational necessity and benefits of information/cyber security governance. They include increased predictability and the reduction of uncertainty in business operations, a level of assurance that critical decisions are not based on faulty information, enabling efficient and effective risk management, protection from the increasing potential for legal liability, process improvement, reduced losses from security-related events and prevention of catastrophic consequences and improved reputation in the market and among customers.

3.2 Information/cyber-Security:

Information/cyber-Security is ensuring information and communications systems and the information are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

The information/cyber security guidelines shall cover security aspects pertaining to network, application, and data/information apart from security awareness to the users. Unitech Plasto Components does not have a customer interface and does not deal with sensitive customer data. Hence, the requirements of cyber security will be adhered to keeping in view the IT system environment of Unitech Plasto Components and the applicability of various requirements.

Unitech Plasto Components shall take effective measures to prevent cyber-attacks and to promptly detect any cyber-intrusions so as to respond / recover / contain the fall out.

3.3 Awareness and Training:

Managing cyber risk requires the commitment of the entire organization to create a cyber-safe environment. This will require a high level of awareness among staff at all levels at Unitech Plasto Components. All staffs of Unitech Plasto Components and, where relevant, contractors and third-party users shall receive appropriate awareness training and regular updates in organisational policies and procedures, as relevant for their job function. The awareness programme shall be periodically updated keeping in view changes in information/cyber technology system, threats/vulnerabilities and/or the information/cyber security framework. There shall be a mechanism to track the effectiveness of training programmes through an assessment / testing process.

3.4 Business Continuity Planning (BCP) and Disaster Recovery:

Disaster recovery planning is a process that includes performing risk assessment, developing recovery strategies and data backup in case of a disaster. Unitech Plasto Components shall have a business continuity plan and disaster recovery plan to resume normal business operations as quickly as possible after a disaster.

3.4 IT Risk Assessment

Unitech Plasto Components shall undertake a comprehensive risk assessment of their IT systems on a yearly basis, keeping in mind of organizational and compliance requirements. The assessment shall analyse the threats and vulnerabilities to the information technology assets of the organisation and its existing security controls and processes.

3.5 Information Systems Audit

The objective of the Information/Cyber Security Audit is to provide an insight on the effectiveness of controls that are in place to ensure confidentiality, integrity and availability of the organization's IT infrastructure. Information/Cyber Audit shall identify risks and methods to mitigate risk arising out of IT infrastructure such as server architecture, local area networks, physical and information security, telecommunications, etc. Information Security Audit forms an integral part of Internal Audit system of the organisation. The organisation shall have adequately skilled personnel in Audit Committee who can understand the results of the Information Security Audit.

4. Roles and Responsibilities:

The roles and responsibilities of the various stakeholders pertaining to the IT Policy are as follows,

4.1 Managing Director:

Approving the IT Policy

4.2 Information Security Committee:

Members of the Committee – Managing Director, IT Team Department Personnel and Heads of the Department.

- Developing and facilitating the implementation of information security policies, and procedures to ensure that all identified risks.
- Reviewing the position of security incidents and various information security assessments and monitoring activities.
- Reviewing the status of security awareness programs
- Assessing new developments or issues relating to information security

- Reporting to the Managing Directors on information security activities
- Conducting regular ISC meetings (at least once in 6 months) and maintenance of MOM.

4.3 End Users:

- Responsible and accountable for activities associated with an assigned account, as well as assigned equipment and removable media.
- .Protect secrecy of passwords and Business Information
- Report known or suspected security incidents

5. Policies and Procedures:

5.1 Access Control Policy

Data must have sufficient granularity to allow the appropriate authorised access. There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorised purposes. This balance should be recognised. The Access Control Policy addresses this need.

5.2 E-mail Security Policy

Unitech Plasto Components shall implement effective systems and procedures to ensure that e-mails are used as an efficient mode of business communication and implement control procedures so that the email facility is not misused by the users. It also needs to be ensured that e-mail service and operations remain secure, efficient while communicating within intranet as well as through the internet.

5.3 Password Security Policy

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords and the frequency of change. All Application software in Unitech Plasto Components will have to comply with minimum password standards as specified in this document.

5.4 Anti-Virus Policy Virus

Trojans, Worms, etc., are malicious programs called malware and can corrupt or destroy data or may spread confidential information to unauthorised recipients, resulting in loss of Confidentiality, Integrity, and availability of the information. Malware detection and prevention measures as appropriate need to be implemented. The basis of protection against Malware should be founded on good security awareness and appropriate system access controls. The Anti-Virus policy has been framed on the above grounds.

5.5 Network Security Policy:

Appropriate controls should be established to ensure security of data in private and public networks, and the protection of connected services from unauthorised access. Unitech Plasto Components Network infrastructure needs to be protected from unauthorised access. A range of security controls is required in computer networks to protect these environments. Considering the above, the network security policy has been framed for Unitech Plasto Components.

6. Compliance:

Information processing facilities shall be used as per information security policy and acceptable usage policy

- While Unitech Plasto Components respects the privacy of its staffs it reserves the right to audit and/or monitor the activities of its staffs and information stored, processed, transmitted or handled on any assets/devices/services used by staff.
- Exception to security policy and procedure shall be approved through the exception management process.
- Policy exceptions shall be reviewed at least annually and as deemed necessary based on security risks envisaged, emerging threats etc.
- Violations or any attempted violations of security policies and procedures shall result in disciplinary/legal actions