IT and Security Policies are the set of rules, standards, and procedures established by an organization to protect its digital infrastructure, data, systems, and technological resources from unauthorized access, misuse, loss, or cyber threats while ensuring safe and efficient use of company technology by employees. These policies define how employees should properly use company-provided assets such as laptops, desktops, servers, email accounts, cloud platforms, databases, internal networks, and software tools, and they enforce strict guidelines for password management, multi-factor authentication, secure login practices, and periodic credential updates to prevent breaches. They regulate internet and email usage by restricting access to unsafe or non-work-related websites, prohibiting illegal downloads, and preventing phishing or malware attacks. Data protection rules specify how sensitive information such as customer data, project files, intellectual property, financial records, and confidential documents must be stored, shared, encrypted, or backed up, along with rules against copying data to personal devices or external drives. IT security policies also include confidentiality agreements (NDAs), access control mechanisms based on roles and responsibilities, monitoring of system activities, firewall and antivirus protections, and incident response procedures in case of cyberattacks or data leaks. Additionally, they cover remote work security practices like VPN usage, secure Wi-Fi connections, device locking, and restrictions on public networks to maintain protection outside the office. Bring Your Own Device (BYOD) rules, software installation restrictions, regular system updates, and compliance with cybersecurity standards are also defined to maintain system integrity. Violations such as sharing passwords, installing unauthorized applications, or leaking company data may lead to disciplinary or legal action. Overall, IT and Security policies ensure confidentiality, integrity, and availability of organizational information while creating a secure digital environment that protects both the company and employees from technological risks.