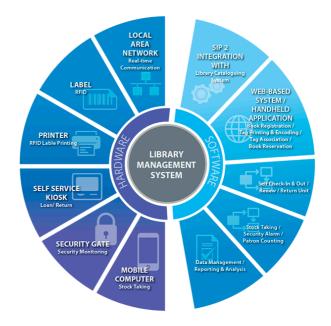
Content and Library Management



Specification

Key Features

- Access Control: Implementing strong access controls to ensure that only authorized personnel and users can access certain content and resources. This includes using usernames and passwords, biometric authentication, or access cards.
- Data Encryption: Ensuring that sensitive data, including user information and library materials, is encrypted both in transit and at rest to protect against unauthorized access.
- Regular Audits and Monitoring:
 Conducting regular security audits and continuously monitoring systems for unusual activity helps to identify potential security breaches quickly.
- Software Updates: Keeping all software and systems updated to protect against vulnerabilities that can be exploited by malicious actors.
- Backup and Recovery: Establishing a robust data backup and recovery plan to prevent data loss in case of a security breach or system failure.
- Incident Response Plan: Developing and maintaining an incident response plan to effectively handle any security breaches that occur, minimizing damage and restoring security promptly.
- Physical Security: Ensuring that the physical premises of the library or content management system are secure, including surveillance cameras, security personnel, and secure access points.



INP TECHNOLOGIES PVT. LTD.