Shriram Properties
Homes that live in you

IT POLICY

Shriram Properties Limited (SPL) is committed to maintaining the highest standards of information and data protection security. This policy outlines our approach to safeguarding sensitive information and data assets from unauthorized access, disclosure, alteration, or destruction. Our dedication to security ensures the confidentiality, integrity, and availability of information, supporting our business operations and the trust of our clients.This policy applies to all employees, contractors, partners, and third-party vendors who handle or have access to Shriram Properties Limited (SPL) information and data assets

POLICY PRINCIPLES

Data Classification and Handling:

- All information and data assets shall be classified based on their sensitivity and criticality.
- Employees must follow proper data handling procedures, ensuring appropriate security measures are applied to each classification level.

Access Control and Authorization:

- Access to information and data assets will be granted on a need-to-know basis.
- User access rights shall be reviewed regularly and promptly revoked upon job role changes or termination.

Authentication and Identity Management:

- Strong authentication mechanisms, such as multi-factor authentication (MFA), shall be implemented for accessing sensitive systems and data.
- User identities will be managed through a centralized system to ensure accurate and secure authentication.

Network and System Security:

- Robust firewall and intrusion detection/prevention systems will be deployed to protect against unauthorized network access.
- Regular security assessments and vulnerability scans will be conducted to identify and mitigate potential risks.

Incident Management and Response:

- An incident response plan will be maintained to handle security breaches, data breaches, and other security incidents promptly and effectively.
- All incidents shall be reported to the designated security team for assessment, mitigation, and resolution.

Physical Security:

- Access to physical locations housing information and data assets shall be restricted to authorized personnel only.
- Surveillance systems and access control mechanisms will be employed to enhance physical security.

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract. For questions or concerns regarding this policy, please contact SPL-IT