

Information Security (IS) Policy

Purpose

To safeguard the organisation's information assets, IT infrastructure, and client data against unauthorized access, breaches, and misuse.

Scope

Applicable to all employees, contractors, interns, and third-party vendors who have access to organisational information systems.

Key Elements

Access Control: Role-based access, password policies, multi-factor authentication, and timely revocation upon exit.

Data Protection: Confidentiality of client and business data, encryption standards, and restrictions on external sharing.

Use of IT Resources: Acceptable use of company hardware, email, internet, and software.

Incident Reporting: Immediate reporting of data breaches, phishing attempts, malware, or suspicious activities.

Remote Work Guidelines: Secure VPN usage, restricted use of personal devices, and compliance with security protocols.

Physical Security: Controlled access to premises, visitor management, and safe storage of sensitive documents.

Compliance: Adherence to applicable IT laws, data protection regulations (such as GDPR, IT Act, etc.), and industry standards.