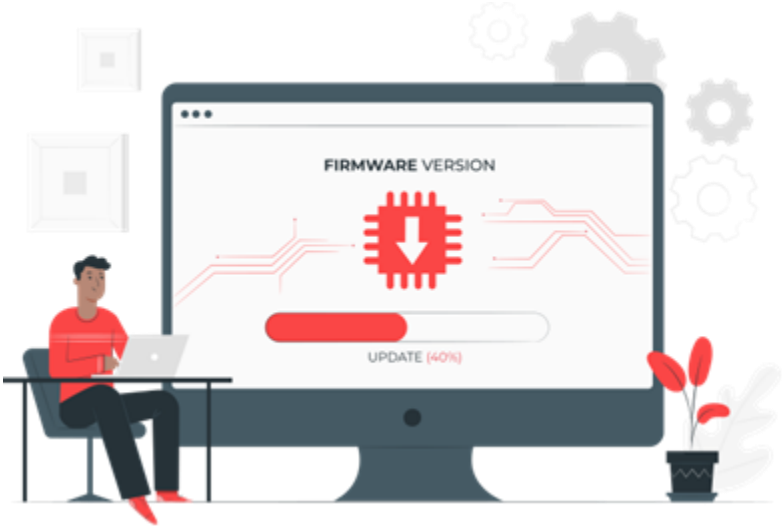

IT and Communication Systems Usage

Acuiti Labs provides IT and communication systems to support business operations. Employees must use these resources responsibly and in accordance with company policies.

Key Guidelines:

Authorized Use: IT and communication systems should be used for business purposes only. Personal use should be minimal and not interfere with work duties.

Security: Protect company data and systems by using strong passwords, encrypting sensitive information, and following security protocols.

Internet and Email: Use the internet and email responsibly. Do not access, download, or distribute inappropriate or unauthorized content.

Software and Hardware: Install and use only authorized software and hardware. Report any issues or malfunctions to the IT department.

Data Protection:

- **Confidentiality:** Maintain the confidentiality of company data. Do not share sensitive information without proper authorization.
- **Data Retention:** Follow company policies on data retention and disposal to ensure compliance with legal and regulatory requirements.

Monitoring:

- **System Monitoring:** The company may monitor IT and communication systems to ensure compliance with policies and protect against security threats.
- **Privacy:** Employees should not expect privacy when using company IT and communication systems.

Security Policies

- Acuiti Labs is committed to maintaining a secure workplace to protect employees, clients, and company assets.

Key Principles:

- **Access Control:** Access to company premises and sensitive areas is restricted to authorized personnel. Employees must use their ID badges to gain access and must not share their credentials with others.
- **Visitor Management:** All visitors must sign in at the reception and be escorted by an authorized employee. Visitors should wear visitor badges at all times while on company premises.
- **Physical Security:** Secure all physical assets, including equipment and confidential documents. Lock offices and cabinets when not in use.
- **Cybersecurity:** Follow cybersecurity best practices to protect against data breaches and cyber threats. Report any suspicious activity or security incidents to the IT department immediately.

Emergency Response:

- **Incident Reporting:** Report any security incidents or breaches to the security team or HR department immediately.
- **Crisis Management:** The company has a crisis management plan in place to respond to security threats, including evacuation procedures, communication protocols, and recovery plans.

Employee Responsibilities:

- **Vigilance:** Be vigilant and report any suspicious behavior or activity.
- **Compliance:** Adhere to all security policies and procedures to ensure the safety and security of the workplace.