Finaleap finserv
FINALEAP FINSERV PRIVATE LIMITED
CIN - U67110PN2021PTC198566 I GST - 27AAECF4558P1ZZ
Office No : O-206, Green Center, Sr. No. 22/1/, Opp. Pune MH 411033.
+91 - 20 - 40022163 info@finaleap.com
www.finaleap.com

FINALEAP FINSERV PRIVATE LIMITED

Information Technology (IT) and Use of Hardware Policy

1. Introduction: This IT and Use of Hardware Policy (hereafter referred to as "Policy") outlines the guidelines and procedures related to the use of information technology resources and hardware at Finaleap Finserv Private Limited (hereafter referred to as "the Company"). This Policy applies to all employees, contractors, and authorized users who access, use, or manage the Company's IT resources and hardware.

2. 2. Purpose: The purpose of this Policy is to Ensure the secure, efficient, and ethical use of the Company's IT resources and hardware. Safeguard the confidentiality, integrity, and availability of sensitive information. Promote responsible and compliant IT practices in line with regulatory requirements, including those stipulated by the Reserve Bank of India (RBI).

3. Scope: This Policy applies to all IT resources and hardware owned or provided by the Company, including but not limited to:
    - Computer systems (desktops, laptops, servers)
    - Mobile devices (smartphones, tablets)
    - Network infrastructure
    - Peripherals (printers, scanners)
    - Software applications and licenses
    - Cloud-based services
    - Data storage and backup solution

4. Responsibilities:

4.1. IT Department: The IT department is responsible for maintaining the integrity and security of IT resources and hardware. Ensuring regular system updates and security patches are applied. Providing technical support to employees and addressing IT-related issues promptly. Conducting regular IT training and awareness programs for employees.

4.2. Employees and Authorized Users: Employees and authorized users are responsible for Adhering to this Policy and any other relevant IT-related policies. Using IT resources and hardware for legitimate business purposes only. Safeguarding login credentials and using strong passwords. Reporting any suspected security incidents or breaches to the IT department.

5. Acceptable Use of IT Resources and Hardware:

5.1. Authorized Use: IT resources and hardware must be used solely for legitimate business purposes related to the Company's operations. Personal use should be limited to reasonable and non-disruptive levels.

5.2. Software Usage: Employees must only install authorized and licensed software approved by the IT department. Unauthorized installation or distribution of software is strictly prohibited.

5.3. Data Security: Employees must follow data security measures, including Refraining from sharing sensitive data externally without proper authorization. Encrypting sensitive information when transmitting over public networks. Adhering to data classification guidelines and access controls.

6. Protection of IT Resources and Hardware:

6.1. Security Measures: All IT resources and hardware must be protected from unauthorized access, loss, damage, or theft. Employees should lock their workstations when leaving their desks unattended.

6.2. Physical Security: Access to data centers, server rooms, and other critical IT infrastructure areas must be restricted to authorized personnel only.

7. Reporting Security Incidents: Employees must promptly report any suspected security incidents, such as unauthorized access, malware infections, or lost/stolen hardware, to the IT department.

8. Allotment of Email IDs

8.1. Eligibility: Official email IDs will be allotted to employees who meet the following criteria:
- Regular full-time employees
- Part-time employees with a minimum commitment of [Insert minimum hours]
- Contractual employees engaged for a duration of [Insert minimum duration]

8.2. Format: Email IDs will follow a standard format, typically based on the employee's name or a combination of the name and designation. The IT department will determine the format to ensure consistency and ease of identification.

8.3. Issuance: Upon completion of the on boarding process or as part of the employee's orientation, the HR department or designated personnel will request the IT department to issue an official email ID to the eligible employee.

8.4. Password Security: Employees will receive login credentials and are responsible for maintaining the confidentiality of their email account passwords. Strong password practices must be followed, including regular password changes.

9. Surrender of Email IDs:

9.1 Termination of Employment: Upon termination of employment, whether voluntary or involuntary, the employee's email ID will be deactivated immediately to prevent unauthorized access to company resources.

9.2 Resignation or Transfer: In the case of an employee's resignation or transfer to another department within the Company, the HR department or designated personnel will inform the IT department in advance. The employee's email ID will be transferred or deactivated, depending on the situation.

9.3 Return of Company Assets: Along with the surrender of the email ID, employees are required to return all company-owned hardware, software, and data storage devices in their possession.

10. Data Retention and Backup:

10.1. Data Retention: The Company reserves the right to retain a copy of email data for a specific period as per its data retention policy and applicable legal requirements.

10.2. Backup: Regular backups of email data will be performed to ensure data integrity and recovery in case of any unforeseen incidents.

11. Monitoring: The IT department will monitor email usage to ensure compliance with this policy and relevant regulations. Unauthorized or inappropriate use of email IDs will be subject to disciplinary action as per the Company's policies.

12. Compliance and Audit: The Company reserves the right to audit and monitor IT resources and hardware usage to ensure compliance with this Policy and applicable regulations.

13. Policy Violations and Consequences: Non-compliance with this Policy may result in disciplinary action, up to and including termination of employment or contract. Legal and regulatory consequences may also apply.

14. Policy Review: This Policy will be reviewed and updated as required, considering changes in technology, regulatory requirements, and business needs.

15. Acknowledgment: By using the Company's IT resources and hardware, employees and authorized users acknowledge that they have read, understood, and agreed to comply with this Policy.