



सत्यमेव जयते

INDIA NON JUDICIAL

Government of Tamil Nadu

e-Stamp

Certificate No. : IN-TN68697076002796U
Certificate Issued Date : 28-Nov-2022 03:31 PM
Account Reference : NEWIMPACC (SV)/ tn8023904/ SEMBIAM/ TN-CN
Unique Doc. Reference : SUBIN-TNTN802390469168333489042U
Purchased by : CredAvenue Private Limited
Description of Document : Article 5 Agreement
Property Description : Employment Agreement
Consideration Price (Rs.) : 0
(Zero)
First Party : CredAvenue Private Limited
Second Party : Employee
Stamp Duty Paid By : CredAvenue Private Limited
Stamp Duty Amount(Rs.) : 50
(Fifty only)



Please write or type below this line

IN-TN68697076002796U

JD 0012789008

Statutory Alert:

1. The authenticity of this Stamp certificate should be verified at www.shcisstamp.com or using e-Stamp Mobile App of Stock Holding. Any discrepancy in the details on this Certificate and as available on the website / Mobile App renders it invalid.
2. The onus of checking the legitimacy is on the users of the certificate.
3. In case of any discrepancy please inform the Competent Authority.

Harish B

22-Feb-2023

Employment Contract

Dear Harish,

We wish to formalize our Offer of Appointment (“**Appointment Letter**”) at **CredAvenue Private Limited, under its brand “Yubi™” (“Company”)** with you. This will be with effect from **22-Feb-2023** on the terms and conditions mentioned below. This Appointment Letter is highly confidential between you and the Company and any disclosure of the same to any third person will lead to disciplinary action by revocation of this Appointment Letter or termination if found thereafter.

1. Selection criteria

- 1.1 Your selection has been made on the basis of information and representations provided by you which the Company assumes to be true, correct, and genuine.
- 1.2 We also reserve the right to take references from your ex-employers and from any other persons whose references have been mentioned in your resume and application form.
- 1.3 If at all, at any time in future, it is found that you have concealed any information or misrepresented the facts, this Appointment Letter shall be terminated by the Company with immediate effect.

2. Position in company

- 2.1 You will be employed on a permanent full-time basis in the **Software Quality - CAPL** team as **Sr. SDET - CAPL** based at **Chennai_TE_CAPL** in accordance with the rules of the Company for the time being in force and as amended from time to time.

3. Commencement of work

- 3.1 Your services to the Company will commence from **22-Feb-2023** (commencement date).

4. Remuneration

- 4.1 The details are attached in Annexure – I
- 4.2 **Payment mode:**
 - 4.2.1 The remuneration will be deposited in your bank account which we have a tie up with. In case you do not hold an account with the designated bank, the Company will help you open a new account.
- 4.3 **Reimbursement:**
 - 4.3.1 The Company will reimburse you for any reasonable expenses properly incurred in carrying out the duties at actuals in accordance with this Appointment Letter, subject to production of satisfactory evidence.

5. Duties

- 5.1 You are required to perform the duties as advised to you at the time of joining. The Key Responsibility Area (KRA) for performing your duties will be set by your Reporting Manager and duties will be carried out accordingly.
- 5.2 These duties may change or be diversified by the Company depending on your skills and competencies.
- 5.3 In addition to performing your duty, you must
 - 5.3.1 carry out all lawful and reasonable instructions given to you by the Company in relation to your employment.
 - 5.3.2 serve the Company faithfully, efficiently, and diligently and exercise all due care and skill in the performance of your duties.
 - 5.3.3 refrain from acting or giving the appearance of acting contrary to the interests of the Company.
 - 5.3.4 carry out any other duties reasonably required by the Company to the best of your skills and abilities and adhere to the Company's policies.

6. Responsibilities

- 6.1 You should keep the Company informed about any change in your personal, professional information and other such relevant information. The Company will have the right to share necessary and relevant information to third parties and as required by law.

7. Hours of Work

- 7.1 You will be required to work for reasonable hours as required by your role.
 - 7.1.1 Your hours of attendance shall be regulated to suit the duties entrusted to you from time to time as required by the management of the Company.
 - 7.1.2 You will be required to work generally for nine hours a day i.e., 09:30 to 18:30, for a stipulated number of days in a week, as per the department that you would be a part of, during the course of your employment.
- 7.2 Your remuneration is compensated to you for all time worked. As such, you will not be entitled to additional payment for additional hours worked.

8. Leave

- 8.1 You will be entitled to leaves as per the leave policy of the Company.
- 8.2 The application of leave and you availing it, is subject to leave policy for the time being in force and as amended from time to time. The details of such leave policy will be made available to you on your acceptance of this Appointment Letter.

9. Retirement

- 9.1 Your employment with the Company will terminate under Clause 15 of this Appointment Letter or retirement whichever is earlier. In any case, you will retire by the age of 60 i.e., on the last day of the month of your 60th birthday.

10. Policies and Procedures

- 10.1** The Company, in order to comply with its legal obligations and to keep up with best practises, may from time to time introduce policies and procedures.
- 10.2** By accepting this Appointment Letter, you agree to read, become familiar and adhere with such policies and procedures and comply with them and encourage others to do likewise.
- 10.3** The facilities and amenities granted to you by these policies and procedures to perform your duties in excess of the statutory requirements do not form part of the conditions of service and subject to change at the discretion of the management.

11. Occupational Health and Safety

- 11.1** You must comply with, and ensure that others also comply with, all Company procedures and policies and all of the Company's reasonable instructions, relating to occupational health and safety in order to protect both your own health and safety and the health and safety of other employees, contractors, the public and any other person having dealings with the Company.
- 11.2** You must not take (or possess) non-prescribed drugs or alcohol while at work. You must inform us, prior to commencing work, if you are under the influence of drugs (prescribed or non-prescribed), alcohol or any other substance including but not limited to any kind of intoxicating substances likely to affect your ability to work.

12. Intellectual Property

You acknowledge and agree that all intellectual property discovered or developed by you during the course of your employment shall belong exclusively to the Company (even after the cessation of your employment) in accordance with the Non-Disclosure Agreement executed with you and the Company, and to the extent such rights do not vest with the Company, you hereby assign to the Company, on an irrevocable, unconditional, perpetual and worldwide basis, all rights, title and interest in such intellectual property. No such rights shall lapse based on the Company's non-exercise of the same.

13. Confidentiality

- 13.1** In accordance with the Non-Disclosure Agreement, you agree that during your employment in the Company, you will have access to confidential information of the Company.
- 13.2** During your employment in the Company and following the cessation of that employment you agree that you:
 - 13.2.1** will not disclose to any third party any confidential Information.
 - 13.2.2** will not use or attempt to use any confidential Information in any manner which is not in the proper course of your duties and for the sole benefit of the Company or its affiliates, subsidiaries and
 - 13.2.3** will use your best endeavours to maintain the secrecy of and prevent the disclosure of any such confidential Information to third parties.
 - 13.2.4** You also agree to sign and execute any and all Non-Disclosure Agreement which will contain detailed obligations in relation to protection of confidential information as and when requested by the Company. You will be bound by the terms of the Non-Disclosure Agreement and if there is any conflict or inconsistency between this Appointment Letter and the Non-Disclosure Agreement, the Non-Disclosure Agreement shall prevail to the extent of such conflict or inconsistency.

14. Transferability

- 14.1** You can be transferred to any of the Company's subsidiaries, establishments, branches, units, work places situated in any part of India. On your transfer, you will be governed by the Company's rules applicable to that establishment.

15. Termination

- 15.1** Either the Company or you may terminate your employment at any time, without assigning any reasons, by providing **sixty (60) days'** written notice or payment of the amount (equivalent to sixty days remuneration) in lieu thereof. However considering that during the course of your employment with the Company, you shall be privy to or shall otherwise have access to sensitive and confidential information of the Company, which may include but not be limited to products' related information for existing or conceived products, business plans, information related to existing and planned projects, vendors and partners' related information and other valuable information of the Company or you may be or needed to be engaged in a project that needs to be completed or for the needs of other business reasons/requirements, in the event you choose to terminate your employment with the Company, the Company shall have the right to refuse acceptance of **sixty (60) days'** salary in lieu of notice period and (i) require you to continue to serve the Company during the notice period or any part thereof, OR (ii) for the duration of the notice period or any part thereof, require that you do not perform any official duties or attend office and return all assets provided by the Company, provided however that during such notice period or part thereof, you shall not take up employment or any other engagement (including as a consultant or advisor), whether on a full time or part time basis, with any other person or entity.

- 15.2** Your employment shall stand terminated forthwith unless otherwise intimated by the Company on the happening of the following:

- 15.2.1** If you are guilty of Serious misconduct of such a nature that it would be unreasonable for the Company to continue your employment during the required period of notice.

For the purpose of this clause/ Appointment Letter, term "Serious misconduct" shall include but not limited to the following:

- 15.2.2** wilful or deliberate, behaviour by you that is inconsistent with the continuation of the Appointment Letter.
- 15.2.3** conduct that causes imminent, and serious, risk to the health, or safety, of a person or the Company's business.
- 15.2.4** you are engaging in theft or fraud or assault.
- 15.2.5** breach of your obligations under Clauses 12, 13 and 16 of this Appointment Letter.
- 15.2.6** you being intoxicated at work; or
- 15.2.7** you refusing to carry out a lawful and reasonable instruction.

- 15.3** Upon cessation of this Appointment Letter, for whatever reason, you must return to the Company, as soon as possible and practical (and not later than 7(seven) calendar days), all property in your possession or control that belongs to the Company This property includes but is not limited to Confidential Information, whether in soft copy or hard copy, and (where applicable) computer, mobile phone, and motor vehicle. The payment of your final dues and provision of any exit documentation from the Company shall be subject to your compliance with this Sub-Clause.

- 15.4** The Company reserves the right to terminate your employment without notice or any payment in lieu thereof "for cause" if you are found to be guilty of any offence under any law for the time

being in force in any jurisdiction involving moral turpitude, misconduct, indiscipline, negligence in your duties, violation of the Company's policies, or should you undertake any form of employment or conflicting business activities outside the Company, if you do not have the mental or physical capacity to carry out your official functions, responsibilities or duties; or if you commit any act detrimental to the interests of the Company. If any information furnished by you in your application for employment or during the selection process or at any time during your employment with the Company, is found to be incorrect, and/or if you have suppressed or not disclosed information including with respect to your qualifications, experience, health and/or any other relevant information, the Company may terminate your services without notice or compensation.

16. Restrictive Covenant

- 16.1** You shall devote all of your professional time to the management and operations of the Company during your employment and shall not engage directly or indirectly in any trade or business or profession outside the Company, or undertake any other employment, or undertake business, with or without any commercial gain, except to the extent permitted by the Company. Breach of this condition shall lead to immediate termination of your services by the Company without any notice or compensation in lieu thereof.
- 16.2** You acknowledge that you will be exposed to confidential information of the Company. You further acknowledge that you working with or setting up an establishment carrying out similar activities as the Company will inevitably result in the use/disclosure of Confidential Information prejudicial to the interests of the Company. Therefore, during your employment and for a period of 1 (one) year following the cessation of employment, you agree that you shall not, without the prior written consent of the Company, directly or indirectly (including through your immediate family members), either as an individual on your own account or as a shareholder, director, officer, employee, partner, representative, lender, guarantor, distributor, advisor, consultant or in a similar capacity or function, whether in India or abroad:
- 16.2.1** carry on, own, manage, operate, join, assist, enable, have an interest in, control or otherwise engage or participate in a business similar to that of the Company or be connected in any entity which directly or indirectly is engaged in the business of the Company (including any such business that the Company becomes involved in during your employment with the Company) or competes with the Company.
 - 16.2.2** be involved or become involved or engage in any other activities that may conflict with the obligations to the Company or adversely impact the Company's goodwill.
 - 16.2.3** on your own account or as an agent of any person canvass or solicit for any business competing with the Company.
 - 16.2.4** solicit, endeavour to solicit, influence or attempt to influence any client, vendor, supplier or customer of the Company or any other person to cease doing business with the Company, or with a view to direct their purchase of the Company's products and/or services/business to himself or any person, firm, corporation, institution or other entity in competition with the business of the Company;
 - 16.2.5** solicit or attempt to influence any person employed or engaged by the Company to terminate or otherwise cease such employment or engagement with the Company;
 - 16.2.6** hire any person who was employed or engaged by the Company at any time while you were employed with the Company;
 - 16.2.7** counsel or procure any person or entity to do any of the foregoing.
- 16.3** You acknowledge that the above restrictions are in the circumstances reasonable and necessary to protect the Company's legitimate business interests and goodwill. In the event of breach or threatened breach of the covenant set forth in this Clause, you understand that the Company will suffer irreparable harm and therefore, the Company will be entitled to an injunction restraining you from committing such breach and/or claim for damages. Nothing contained herein shall be

construed as prohibiting the Company from pursuing any other remedies available to it for such breach or threatened breach.

- 16.4** If any such restriction(s) under this Clause is found to be void, but would be valid if some part thereof was deleted or the scope, period or area of application were reduced, such restriction(s) shall apply with the deletion of such words or such reduction of scope, period or area of application as may be required to make the restriction(s) contained in this Clause valid and enforceable. Notwithstanding the limitation of this provision under applicable laws, the parties undertake to, at all times, observe and be bound by the spirit of this Clause. Provided however, that on the revocation, removal or diminution of the relevant law or restriction, as the case may be, by virtue of which the original restrictions contained in this Clause were limited, such original restrictions would stand renewed and be effective to their original extent, as if they had not been limited by the law or restrictions revoked.
- 16.5** It is agreed by and between the parties that the employment with the Company and the compensation payable under this Appointment Letter shall be sufficient consideration for this Clause.

17. General Provisions

- 17.1** The validity, interpretation and performance of this Appointment Letter will be governed by the law of India. Subject to the terms of Clause 18, the parties submit to the non-exclusive jurisdiction of the Courts of Chennai in respect of any dispute that arises in connection with this Appointment Letter.
- 17.2** This Appointment Letter and any Non-Disclosure Agreement executed between the parties contains the entire understanding between the parties in relation to its subject matter. There are no express or implied conditions, warranties, promises, representations or obligations, written or oral, in relation to this Appointment Letter other than those as expressly stated in it or necessarily implied by law.
- 17.3** You acknowledge that you have entered into this Appointment Letter without relying on any representation by the Company.
- 17.4** No failure, delay, relaxation or indulgence by a party in exercising any power or right conferred upon it under this Appointment Letter will operate as a waiver of that power or right. No single or partial exercise of any power or right precludes any other or future exercise of it, or the exercise of any other power or right under this Appointment.
- 17.5** If any provision of this Appointment Letter is invalid, void or unenforceable, all other provisions which are capable of separate enforcement without regard to an invalid, void or unenforceable provision are and will continue to be of full force and effect in accordance with their terms.
- 17.6** This Appointment Letter binds and inures for the benefit of the parties, their respective successors (including, in the case of natural persons, their legal personal representatives) and permitted assigns.
- 17.7** A notice or other communication will be taken for the purposes of this Appointment Letter, to have been given if:
- 17.7.1** Personally delivered, upon delivery;
 - 17.7.2** mailed, on the expiration of two Business Days after posting;
 - 17.7.3** sent by facsimile transmission, on the day it is sent (or, if that is not a Business Day, on the next Business Day); or
 - 17.7.4** sent by e-mail, when the recipient sends an acknowledgment of receipt of the e-mail.

- 17.8** You may not without the prior written consent of the Company assign or encumber all or any part of his rights under this Appointment Letter or attempt or purport to allow another person to assume your obligations under this Appointment Letter.
- 17.9** On execution of this Appointment Letter, all previous Appointments Letter between the above two parties stand void.
- 17.10** In the event of cessation of your employment, you consent to the Company notifying any new employer and/or any third party about your continuing obligations under this Appointment Letter. If necessary, the Company has a right to disclose this Appointment Letter to any new employer or third parties.

18. Arbitration

If any dispute arises between you and the Company with respect to this Appointment Letter, the parties to this Appointment Letter shall first endeavour to co-operate to resolve the dispute or controversy by mutual consultation. All disputes, claims arising out of this Appointment Letter shall be referred to the Arbitration of a sole arbitrator who has been appointed mutually by you and the Company under the Arbitration and Conciliation Act, 1996 or any statutory modifications made thereof from time to time. The venue for the arbitration shall be in Chennai, India, and the parties shall be subject to the jurisdiction of the Courts in India, which shall have exclusive jurisdiction in the proceedings regarding the enforceability of this Appointment Letter to arbitrate.

CREDAVENUE PRIVATE LIMITED

Abhishek Mehrotra

Abhishek Mehrotra (February 27, 2023, 8:26 GMT)

27-Feb-2023

Abhishek Mehrotra

Chief Human Resources
Officer

Agreed & Accepted

Harish Baskaran

Harish Baskaran (February 27, 2023, 8:27 GMT)

27-Feb-2023

Employee Name: Harish B

Annexure 1: Salary Breakup

| COMPENSATION STRUCTURE | |
|-------------------------|--------------------|
| Basic | ₹ 12,50,000 |
| HRA | ₹ 6,25,000 |
| Special Allowance | ₹ 6,25,000 |
| Annual Gross CTC | ₹ 25,00,000 |
| Provident Fund | ₹ 1,50,000 |
| Annual Fixed CTC | ₹ 26,50,000 |

The organisation has the right to change or alter individual components of the salary at any time based on statutory requirements and other organisation policies that may come into place from time to time. The total fixed salary however will remain unchanged

Apart from the financials mentioned, you will be eligible for the below:

- Group medical insurance for you and your dependents as prescribed in the policy.
- You will be covered under our Group Life (10X coverage) and Personal accident (7X coverage) insurance.

NON-DISCLOSURE AGREEMENT

This Non-Disclosure Agreement ("**Agreement**"), made on 27-Feb-2023, is by and between **CredAvenue Private Limited**, a company registered under the Companies Act, 2013 and having its registered office at 12th Floor, Prestige Polygon, No. 471, Annasalai, Nandanam, Chennai, Tamil Nadu 600035, India hereinafter referred to as "**CAPL**"), which expression shall, unless it be repugnant to the context or meaning thereof, be deemed to mean and include its affiliates, subsidiaries, successors-in-business and assigns;

AND

Harish B holding the Employee Number CA1080 and residing at Block N Flat-071 SBIOA Unity Enclave, Mambakkam Taluk Chinglepet District Chennai - 600127 ("**Recipient**").

CAPL and Recipient shall be collectively referred to as "**Parties**" and individually as "**Party**".

WHEREAS

- A. CAPL and its affiliates and subsidiaries shall be collectively referred to as ("**CAPL Group**" and individually as "**CAPL Group Entity**");
- B. Recipient has been employed with the Software Quality - CAPL team/department at CAPL from 22-Feb-2023; and
- C. Parties hereby acknowledge that pursuant to and during the course of employment of the Recipient as mentioned above, CAPL Group, represented by CAPL and/or the CAPL Group entities may disclose certain information to the Recipient in the usual course of the Recipient performing his/her duties.

NOW THEREFORE, in consideration of the aforesaid, the Parties agree as follows:

1. "**Confidential Information**" Recipient hereby acknowledges and understands that the term "Confidential Information" refers to, any data, information or material, whether or not identified as "confidential" or "Trade Secret", of or relating to: (i) the CAPL, its shareholders, CAPL Group, or (ii) clients and customers or potential clients and customers (collectively "Customer(s)") or (iii) technical information, including patent, copyright and other proprietary information, techniques, sketches, drawings, models, inventions, know-how, processes, apparatus, equipment, algorithms, software programs, software source documents, and formulae related to the current, future and proposed products and services of CAPL Group and any of the CAPL Group Entities, or (iv) non-technical information relating to CAPL Group's or any of the CAPL Group Entities' products, including without limitation pricing, margins, merchandising plans and strategies, finances, financial and accounting data and information, suppliers, Customer lists, purchasing data, sales and marketing plans, future business plans and any other information which is proprietary and confidential to CAPL Group or any of the CAPL Group Entities. The term "Trade Secret(s)" includes, but is not limited to, confidential, proprietary, and/or sensitive: formula; software; methodology; model; architecture; pattern; compilation; program; device; method; technique; passwords; sourcing information; drawings; technical or non-technical data and know-how; data sheet; work methodology, manual of the CAPL Group; processes; material concerning finances, sales, purchasing, marketing, accounting, techniques, dealing, partnerships, structuring, transactions; Customer lists; invoices;

reports containing specifically developed information, such as the name, address, phone number, buying history and other traits of Customers, along with any other information that CAPL Group derives a competitive advantage from and that CAPL Group makes reasonable efforts to maintain a secret.

2. **Use and Non-disclosure Obligations:** Recipient acknowledges that Recipient will have access to and be provided with Confidential Information in connection with performing services for CAPL Group. Recipient will maintain in confidence and will not disclose, disseminate or use any Confidential Information, whether or not in written form. The Recipient hereby agrees and undertakes that the Recipient shall treat all Confidential Information with at least the same degree of care as Recipient accords to their own personal confidential information. To ensure the continued confidentiality of the Confidential Information, the Recipient agrees to hold the Confidential Information in strict confidence, in a fiduciary capacity for the benefit of the CAPL Group. Recipient shall not, either during Recipient's employment with CAPL Group or post-cessation of employment, disclose or use for Recipient's own benefit or for the benefit of any other individual or third party, directly or indirectly, any of the Confidential Information, except as such disclosure or use is expressly authorized by CAPL Group in writing.
3. **Exceptions:** The confidentiality and restriction on the use of Confidential Information under this Agreement shall not apply to Confidential Information to the extent that such Confidential Information: is now, or hereafter becomes, through no breach of this Agreement by Recipient, generally known or available to the public; was known to Recipient without an obligation to hold it in confidence prior to the time such Confidential Information was disclosed to Recipient by CAPL Group; or is disclosed or used, as applicable, with the prior written consent of CAPL Group and in accordance with any limitations or conditions on such disclosure or use that may be imposed in such written consent.
4. **Required disclosure:** The confidentiality obligations under this Agreement shall not apply to Confidential Information to the extent that such Confidential Information is required to be disclosed pursuant to the order or requirement of a court, administrative agency, or other authority, or otherwise by operation of applicable law. In the event of such order or requirement, Recipient, if and to the extent permitted by law, shall give CAPL Group written notice thereof and of the Confidential Information that is required to be disclosed, as soon as practicable prior to the disclosure of such Confidential Information so as to enable the CAPL Group to take necessary steps to ensure that disclosures are limited to the extent possible under law. The Recipient shall also provide such assistance as CAPL Group may reasonably request, at CAPL Group's sole expense, in seeking a protective order or other appropriate relief in order to protect the confidentiality of the Confidential Information.
5. **Return or Destroy Confidential Information:** Recipient agrees, immediately upon the cessation of the relationship between Recipient and CAPL Group for any reason or upon earlier request by CAPL Group, to: cease using the Confidential Information (in physical and electronic form); promptly return to CAPL Group or if requested by the CAPL Group destroy all such Confidential Information and any copies thereof; certify in writing (if requested in writing by the CAPL Group) that Recipient has complied with the obligations of this Subsection.
6. **Intellectual Property:**
 - i. **Intellectual Property Rights.** "Intellectual Property Rights" means copyright, patents, know-how, database rights, and rights in trademarks and designs (whether registered or unregistered),

prototypes, drawings, designs, trade secrets, processes, methods, know how, formula, applications for registration, and the right to apply for registration for any of the same and all other intellectual property rights and equivalent forms of protection existing anywhere in the world.

- ii. **IP Materials.** “IP Materials” means all documents, software, photographic or graphic works of any type, any other materials in any medium or format which are created by the Recipient or on behalf of the **Recipient** in the course of performing the Recipient’s duties, whether individually or jointly with others, during the course of the Recipient’s employment and which are protected by or relate to Intellectual Property Rights.
 - iii. The Recipient may only use the Intellectual Property Rights which arise as a result of the Recipient performing its duties under pursuant to its employment and IP Materials, to perform its duties. The **Recipient** agrees not to use the IP Materials for its own gain. Further, the Recipient agrees not to disclose any Intellectual Property Rights which arise as a result of the Recipient performing its duties pursuant to its employment or IP Materials, to any third party without the express written consent of the CAPL Group.
 - iv. The Recipient agrees to sign any documents and do any other act which the CAPL Group may request (at its **expense**) to enable the CAPL Group to make full use of the benefit of this Section. This includes joining in any application which may be made in the CAPL Group’s sole name, for registration of any Intellectual Property Rights. Decisions as to the protection or exploitation of any Intellectual Property Rights shall be at the sole discretion of the CAPL Group. If, as a result of the Recipient’s mental or physical incapacity or for any other reason whatsoever, after the CAPL Group’s reasonable effort to secure the Recipient’s signature on any relevant documents, the CAPL Group is unable to do so, the Recipient hereby irrevocably authorises the CAPL Group and its duly authorized officers to act for and on its behalf.
 - v. The Recipient agrees that the Recipient will transfer immediately to the CAPL Group all IP Materials in its possession or under its control, on cessation of its employment (for whatever reason) or at any **other** time upon the CAPL Group’s request. No copies or other record of any IP Materials may be retained by the Recipient unless the Recipient has prior written consent from the CAPL Group.
 - vi. The Recipient hereby recognises that Intellectual Property Rights similar or related to the Recipient’s business, relating to the Recipient’s activities while working for the CAPL Group and conceived or made by the Recipient, alone or jointly, within 1 (one) year from the date of cessation of his employment with the CAPL Group, shall have been conceived in significant part while employed by the CAPL Group. Accordingly, the Recipient agrees that such Intellectual Property Rights shall be deemed to have been conceived during his employment with the CAPL Group and shall be assigned to the CAPL Group, unless the Recipient establishes the contrary.
 - vii. Nothing contained in this Agreement shall be construed as granting to the Recipient any right or license under any of the CAPL Group’s present or future Intellectual Property Rights, or as granting to the Recipient any right or license to use such Intellectual Property Rights for any purpose other than those purposes expressly stated herein.
 - viii. The Recipient shall indemnify the CAPL Group for any loss, damage, expenses or infringement should he/she **misuse** or allow others to misuse the CAPL Group’s Intellectual Property Rights and IP Materials.
7. **Term and Survival:** Recipient understands that its obligations under this Agreement shall survive

the cessation of its employment with the CAPL Group. Upon termination of any relationship between the Parties, Recipient will promptly deliver to CAPL or the relevant CAPL Group Entity, without retaining any copies, all documents and other materials furnished to Recipient by CAPL or any CAPL Group Entity.

8. **Governing Law:** The Agreement shall be governed in all respects by the laws of India and any dispute arising out of the Agreement shall be subject to courts of competent jurisdiction situated at Chennai, Tamil Nadu.
9. **Injunctive Relief:** The Recipient hereby agrees and acknowledges that a breach of any of the promises or agreements contained herein will result in irreparable and continuing damage to CAPL Group for which there will be no adequate remedy at law, and the CAPL Group represented by CAPL or the relevant CAPL Group Entity (as applicable) shall be entitled to injunctive relief and/or a decree for specific performance, and such other relief as may be proper (including monetary damages if appropriate).
10. **Entire Agreement:** The Agreement read with the Appointment Letter dated 22-Feb-2023 constitutes the entire agreement with respect to the subject matter herein and supersedes all prior or contemporaneous oral or written agreements concerning such matters.
11. **Amendment:** The Agreement may only be changed by mutual agreement of authorized representatives of the Parties in writing.
12. **Joint and Several Benefit:** It is agreed and understood by the Parties that the obligations owed by the Recipient under this Agreement shall be for the joint and several benefit of the CAPL Group and each CAPL Group Entity, each of which shall be entitled to the rights set out in this Agreement to the same extent as if the instant Agreement was executed by the relevant CAPL Group Entity with the Recipient in its sole capacity.

IN WITNESS WHEREOF, the Parties have executed the Agreement by themselves/ through their authorized representatives.

CREDAVENUE PRIVATE LIMITED

Abhishek Mehrotra

Abhishek Mehrotra (February 27, 2023, 9:26 GMT)

27-Feb-2023

Abhishek Mehrotra

Chief Human Resources
Officer

Agreed & Accepted

Harish

Harish Baskaran (February 27, 2023, 9:27 GMT)

27-Feb-2023

Employee Name: Harish B

FORM 'F'

Nomination

To,

I, Harish B

(Name in full here)

whose particulars are given in the statement below, hereby nominate the person(s) mentioned below to receive the gratuity payable after my death as also the gratuity standing to my credit in the event of my death before that amount has become payable, or having become payable has not been paid and direct that the said amount of gratuity shall be paid in proportion indicated against the name(s) of the nominee(s).

1. I hereby certify that the person(s) mentioned is/are a member(s) of my family within the meaning of clause (h) of Section 2 of the Payment of Gratuity Act, 1972.
2. I hereby declare that I have no family within the meaning of clause (h) of Section 2 of the said Act.
3. (a) My father/mother/parents is/are not dependent on me.
(b) My husband's father/mother/parents is/are not dependent on my husband.
4. I have excluded my husband from my family by a notice dated to the controlling authority in terms of the proviso to clause (h) of Section 2 of the said Act.
5. Nomination made herein invalidates my previous nomination.

Nominee(s)

| Name in full with full address of nominee(s) | | Relationship with the employee | Age of nominee | Proportion by which the gratuity will be shared |
|--|--|--------------------------------|----------------|---|
| (1) | | (2) | (3) | (4) |
| 1. | Aswathi Rajasree I Block N Flat-071 SBIOA Unity Enclave, Mambakkam Chennai - 600127 | Wife | 25 | 100 |

Statement

1. Name of employee in full: Harish B
2. Department/Branch/Section where employed: Software Quality - CAPL
3. Post held with Ticket No. or Serial No., if any: CA1080
4. Date of appointment: 22-Feb-2023
5. Permanent address:
Block N Flat-071
SBIOA Unity Enclave,
Mambakkam
Tiruporur Taluk
Chinglepet District
Chennai - 600127

Place: Chennai



Harish Baskaran (February 27, 2023, 9:27 GMT)

Date: 27-Feb-2023

Signature/Thumb-impression of the Employee

Declaration by Witnesses

Nomination signed/thumb-impressed before me

Name in full and full address of witnesses.

Signature of Witnesses.

1. Aswathi Rajasree I
Block N Flat-071
SBIOA Unity Enclave, Mambakkam
Chennai - 600127
2. Baskaran L
Block N Flat-071
SBIOA Unity Enclave, Mambakkam
Chennai - 600127

Place: Chennai

Date: 27-Feb-2023

Certificate by the Employer

Certified that the particulars of the above nomination have been verified and recorded in this establishment.
Employer's Reference No., if any

Abhishek Mehrotra

Abhishek Mehrotra (February 27, 2023, 9:26 GMT)

27-Feb-2023

Date: 27-Feb-2023

Signature of the employer/Officer
authorized Designation



Name and address of the establishment
or rubber stamp thereof.

CredAvenue Private Limited
12th Floor, Prestige Polygon, No. 471,
Annasalai, Nandanam, Chennai, Tamil
Nadu 600035, India

Acknowledgement by the Employee

Received the duplicate copy of nomination in Form 'F' filed by me and duly certified by the employer.

Harish

Harish Baskaran (February 27, 2023, 9:27 GMT)

Date: 27-Feb-2023

Signature of Employee



New Form : 11 - Declaration Form
(To be retained by the employer for future reference)

EMPLOYEES' PROVIDENT FUND ORGANISATION

Employees' Provident Fund Scheme, 1952 (Paragraph 34 & 57) and
Employees' Pension Scheme, 1995 (Paragraph 24)

(Declaration by a person taking up Employment in any Establishment on which EPF Scheme, 1952 and for EPS, 1995 is applicable)

| | | |
|-----|--|---|
| 1. | Name of Member (Aadhar Name) | Harish B |
| 2. | <input type="checkbox"/> Father's Name <input checked="" type="checkbox"/> Spouse's Name (Please tick whichever applicable) | Aswathi Rajasree Iyyappan |
| 3. | Date of Birth (dd/mm/yyyy) | 19/01/1994 |
| 4. | Gender (Male / Female / Transgender) | Male |
| 5. | Marital Status ? (Single/Married/Widow/Widower/Divorcee) | Married |
| 6. | (a) eMail ID | hazz1994@gmail.com |
| | (b) Mobile No (Aadhar Registered) | +91-9445841008 |
| 7. | Whether earlier member of the Employee's Provident Fund Scheme, 1952 ? | No |
| 8. | Whether earlier member of the Employee's Pension Scheme, 1995 ? | No |
| | Previous Employment details ? (If Yes, 7 & 8 details above) | NA |
| 9. | a) Universal Account Number (UAN) | NA |
| | b) Previous PF Account Number | NA |
| | c) Date of Exit from previous Employment ? (dd/mm/yyyy) | NA |
| | d) Scheme Certificate No (If issued) | NA |
| | e) Pension Payment Order (PPO) (If issued) | NA |
| 10. | a) International Worker | No |
| | b) If Yes, state country of origin (name of other country) | NA |
| | c) Passport No. | NA |
| | d) Validity of passport (dd/mm/yyyy) to (dd/mm/yyyy) | NA |
| 11. | KYC Details : (attach self attested copies of following KYC's) | Must Enclose Scan copy for the following documents |
| | a) Bank Account No. & IFS Code | 236001504147 & ICIC0002360 |
| | b) AADHAR Number | 233791988897 |
| | c) Permanent Account Number (PAN), If available | AHRPH0940G |

| | | | | | | |
|-----|--------------------------------|----------------------------|---|--------------------------------------|--|---|
| 12. | First EPF Member Enrolled Date | First Employment EPF Wages | Are you EPF Member before 01/09/2014 | If Yes, EPF Amount Withdrawn? | If Yes, EPS (Pension) Amount Withdrawn? | After Sep 2014 earned EPS (Pension) Amount Withdrawn before Join current Employer? |
| | 27/02/2023 | | No | NA | NA | No |

UNDERTAKING

- 1) Certified that the particulars are true to the best of my knowledge
- 2) I authorise EPFO to use my Aadhar for verification / authentication / eKYC purpose for service delivery
- 3) Kindly transfer the fund and service details, if applicable, from the previous PF account as declared above to the present PF account.
(The transfer would be possible only if the identified KYC details approved by previous employer has been verified by present employer using his Digital Signature)
- 4) In case of changes in above details, the same will be intimated to employer at the earliest.

Date: 27-Feb-2023



Harish Baskaran (February 27, 2023, 8:27 GMT)

Place: Chennai

Signature of Member

DECLARATION BY PRESENT EMPLOYER

- A. The member Mr./Ms./Mrs. Harish B Has joined on 22-Feb-2023 and has been allotted PF Number
B. In case the person was earlier not a member of EPF Scheme, 1952 and EPS, 1995: ((Post allotment of UAN) The UAN allotted or the member is)
C. Please Tick the Appropriate Option: The KYC details of the above member in the JAN database

☐ Have not been uploaded ☐ Have been uploaded but not approved ☐ Have been uploaded and approved with DSC

- D. In case the person was earlier a member of EPF Scheme, 1952 and EPS 1995;

☐ The KYC details of the above member in the UAN database have been approved with Digital Signature Certificate and transfer request has been generated on portal
☐ As the DSC of establishment are not registered with EPFO, the member has been informed to file physical claim (Form-13) for transfer of funds from his previous establishment.

Date: 27-Feb-2023

Signature of Employer with Seal of Establishment



Abhishek Mehrotra (February 27, 2023, 8:26 GMT)

27-Feb-2023

EMPLOYMENT HANDBOOK ACKNOWLEDGEMENT

I hereby acknowledge that I have received Yubi (a.k.a., CredAvenue) Employee Handbook, and I understand that it is my responsibility to read, understand, and comply with the policies contained in this handbook and any revisions made to it. Since the information, policies, and benefits described here are subject to change, I acknowledge that revisions to the handbook may occur and any such changes pertaining to the handbook / HR policies will be communicated officially, and I also understand that revised information may supersede, modify, or eliminate existing policies and only Yubi (a.k.a., CredAvenue) HR can adopt any revisions to the policies in this handbook. I understand that I have a responsibility to check email, policy repository and other forms of communication from Yubi (a.k.a., CredAvenue) to stay informed of any changes made to this handbook / HR policies. I understand that I should consult my manager or HR regarding any questions answered / not answered in the handbook. Furthermore, I acknowledge that this handbook is neither a contract of employment nor a legal document.

Employee Name : Harish B

Signature :



Harish Baskaran (February 27, 2023, 9:27 GMT)

Date : 27-Feb-2023

INDUCTION ACKNOWLEDGEMENT

I hereby acknowledge that, I have attended the Induction Program on Organizational Policies and Procedures including Information Security awareness.

Organizational Policies:

| S No | List of Policies |
|------|---------------------------------------|
| 1 | ISMS User Agreement |
| 2 | Information Security Policy |
| 3 | Data Protection and Security Policy |
| 4 | Privacy Policy |
| 5 | Cyber Security Policy |
| 6 | Acceptable Use policy |
| 7 | Laptop Security policy |
| 8 | Clean Desk and Clean Screen Procedure |
| 9 | Email Procedure |

Employee Name : Harish B

Signature :



Harish Baskaran (February 27, 2023, 9:27 GMT)

Date : 27-Feb-2023

ISMS Document

ISMS User Agreement

Document Control ID: Yubi-ISP-19

Issued Date: 19-10-22

Published Date: 19-10-22

Confidential and Proprietary Information of CredAvenue Private Limited ('Yubi'). Only expressly authorized for individuals under obligations of confidentiality with Yubi are permitted to review materials in this document. By reviewing these materials, you agree to not disclose these materials to any third party unless expressly authorized by CredAvenue Private Limited and to protect the materials as confidential and trade secret information. Any unauthorized review, retransmission, dissemination, or other use of these materials is strictly prohibited. If you are not authorized to review these materials, please return these materials (and any copies) from where they were obtained. All materials found herein are provided "AS IS" and without warranty of any kind.

DOCUMENT AND RECORD CONTROL

Revision Table

| Date | Version | Brief Description | Author |
|-----------------|---------|-----------------------------|--------------------|
| 07-September-21 | 0.1 | ISMS User Agreement – Draft | Abinesh Athilingam |
| 29-September-21 | 1.0 | ISMS User Agreement | Abinesh Athilingam |
| 26-September-22 | 1.1 | Formatting changes | Devika Subbaiah |

Approval History

| Date | Version | Approval | Title |
|-----------------|---------|----------|-------------------------|
| 29-September-21 | 1.0 | Approved | Chief Executive Officer |
| 19-October-22 | 1.1 | Approved | CISO |

Important Note: This document is intended solely for the use of the individual or entity to whom it is transmitted to, and others authorized to receive it. It may contain confidential or legally privileged information. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this document is strictly prohibited and may be unlawful. If you have received this document in error, please notify us immediately.

TABLE OF CONTENTS

| | |
|--|-----------|
| Process Conformance | 5 |
| Acronyms | 5 |
| Computer Misuse | 5 |
| User Accountability | 7 |
| Care of Equipment | 8 |
| Personal Use | 9 |
| Monitoring and Compliance | 10 |
| Protecting Information | 11 |
| Work from Home Policy | 12 |
| Security Reporting | 12 |
| Additional Privileges | 13 |
| Reporting of Security Incidents | 13 |

Yubi ISMS User Agreement

The purpose of this agreement is to define acceptable and unacceptable behavior when using CredAvenue Private Limited ('Yubi') computing facility and to clarify what actions may be taken if the agreement is breached.

1. Process Conformance

| Standard/Model | Clause/Section (Key) Process Area |
|----------------|-----------------------------------|
| ISO 27001:2013 | |
| ISMS Policy | |

2. Acronyms

| Abbreviation | Description |
|---------------------------|--|
| User | Any employee, contractor, consultant, visitor, student, business associate, faculty or any other individual or company who accesses the Information System infrastructure of Yubi from local or remote location. |
| Organization | Yubi |
| IT | Information Technology |
| Outsider | Any individual who is not in the direct role of Yubi. |
| ISMS | Information Security Management System |
| Helpdesk | Central contact point for all the computer users who have computer related queries and technical support service requirements. |
| ISF | Information Security Forum |
| Computing Facility | Yubi computing facilities consist of information processing and storage hardware and software. For Example: Desktops, Computers, Laptops, Intranet, Internet, Emails, Servers, Network Components, etc. |

3. Computer Misuse

| | |
|---------------------------------------|--|
| Computer Misuse | <p>The following section gives some examples of unacceptable behavior that would constitute misuse of Yubi computing facility and therefore lead to disciplinary action and possible dismissal. The list gives examples but is not exhaustive.</p> <p>You must not use your computer system to publish, display, store, request (download) or transmit any information that:</p> <ul style="list-style-type: none"> • Violates or infringes another person's rights. • Contains any defamatory, false, abusive, obscene, profane, sexually orientated, intimidating, threatening, racially offensive, biased or discriminatory material, including where asterisks have been used to 'disguise' words that would otherwise fall under this category. • Forges, impersonates, misrepresents, misleads or fabricates, including representing personal opinions as those of Yubi. • Is malicious, for example, computer viruses, hacking/cracking tools, etc. • May bring Yubi into disrepute, for example engaging in gossip or speculation or expressing derogatory views about people or organizations. • Solicits, encourages or uses the systems for any activity prohibited by law or Yubi policy. • Interferes with the business of Yubi, its customers or suppliers. • Creates a nuisance, for example, by using email for: frequent personal use, sending chain mail or other unsolicited messages such as jokes. • Damages or inhibits efficiency for example, intentionally forwarding large graphics or the unnecessary use of large distribution lists. • Would release company-sensitive information inappropriately. |
| Sexually Explicit Material | <ul style="list-style-type: none"> • The display of any kind of sexually explicit image or document on any company system is a violation of this agreement. In addition, sexually explicit material must not be accessed, attempted to be accessed, archived, stored, distributed, edited or recorded using Yubi network or computing resources. |
| Download of Software and Games | <ul style="list-style-type: none"> • Users with Internet access shall not use company facilities to download entertainment software or games, or to play games against opponents over the Internet. |
| Download of Images and Videos | <ul style="list-style-type: none"> • Users with Internet access shall not use company Internet facilities to download images or videos unless there is an explicit business-related use for the material. |
| Upload of Information | <ul style="list-style-type: none"> • Users with internet access shall not upload any software licensed to Yubi or data owned or licensed by Yubi without explicit authorization from the manager responsible for the software or data. |
| Internet-Based Email | <ul style="list-style-type: none"> • External emails should not be accessed from Company's system |

| | |
|------------------|--|
| Copyright | <ul style="list-style-type: none"> If copyrighted material is used, it must be done so within the terms published by the copyright owner and must not contravene copyright law. |
|------------------|--|

4. User Accountability

| | |
|---|--|
| Accountability | <ul style="list-style-type: none"> You will have a unique login ID and are accountable for all actions attributable to that ID. |
| Password Disclosure | <ul style="list-style-type: none"> For your protection, you are responsible for keeping your personal passwords (including any PINs you are issued) secret. You must change them regularly or when prompted by the system and make new passwords difficult for others to guess. Passwords should contain a mixture of both characters and digits. You should not disclose your password to anyone else, even if you leave the company and you must not use someone else's ID and password. You must change your password immediately if you suspect someone else knows it. An exception to this is that you may need to tell an engineer/systems administrator your password to fix a problem with your computer. If this happens, you should change your password immediately afterwards. You must be diligent in protecting both your password and system by locking your workstation whenever you leave it. The use of shared passwords is not permitted unless a formal business case has been expressly authorized with documented evidence. |
| Unauthorized Modifications and Connections | <ul style="list-style-type: none"> Unless expressly authorized, users must not install, change, move or make any additions to computer systems, including connecting unauthorized computer equipment, for example Personal Digital Assistants (PDAs), USB drives, external HDD/ CD drives, etc., to the Yubi computing facility. |
| External Network Connections | <ul style="list-style-type: none"> Unless expressly authorized, users must not attach a Yubi computer to a non-Yubi network or unauthorized network connection. |
| Interference with Security Software | <ul style="list-style-type: none"> Unless expressly authorized, users must not access, interfere with, switch off, remove or disclose details of security software or codes, including virus protection software (CrowdStrike). |
| Software | <ul style="list-style-type: none"> Users must not knowingly or otherwise load or use unlicensed or unauthorized software. Unauthorized copies of software or information must not be taken, used or transferred from the Internet. |
| Hardware and Software | <ul style="list-style-type: none"> Users will only use approved hardware and software purchased through the IT team. |
| Access to Systems | <ul style="list-style-type: none"> You must not attempt to access any computer system or to use any part of a computer system unless you have been authorized. You must not attempt to use another user's password, privileged system access or a System Administrator's account. |

5. Care of Equipment

| | |
|--------------------------------------|---|
| Computing Equipment | <ul style="list-style-type: none"> • If Yubi supplies you with equipment such as laptops to take out of the workplace, it does so on the strict understanding that it remains the property of Yubi. It may be recalled to the workplace at any time and must be returned if you leave the employment of Yubi. All other restrictions stated in this agreement also apply. • If you take computer equipment out of the office, it must not be left unattended in a public place or be visible in an unattended place. When travelling by air, mobile computing equipment should be carried as hand luggage. • You must be diligent when taking equipment home to keep it safe. • In the event of loss or suspected loss, you should report this to your line manager, Admin and IT department immediately. |
| Access to Computing Equipment | <ul style="list-style-type: none"> • You must not allow unauthorized people to access or use Yubi computer equipment. This includes, but is not limited to, friends, family and suppliers. |
| Personal Computer Equipment | <ul style="list-style-type: none"> • If you use your own personal computer equipment to carry out work for Yubi, you must ensure that up to date virus protection (CrowdStrike) is installed and that you are using licensed software. |

6. Personal Use

| | |
|---------------------------|--|
| Acceptable Use | <p>You are permitted to use general computer systems such as email and Internet access for personal purposes provided that:</p> <ul style="list-style-type: none"> • You do not misuse the systems (see Computer Misuse section above). • It is in your own time (for example lunchtime and outside of your normal working hours), it is infrequent and not excessive and does not interfere with your or another member of staff's work. • Storage of files on your personal drive is kept to a minimum and does not include large file types such as electronic photographs and music. • You do not send images, sound clips or other multimedia files in email messages. • You do not conduct any business affairs not related to Yubi. • You do not order goods (IT products) privately for delivery to Yubi premises. • You do not access and subsequently bid for items on any Internet auction sites using a Yubi email account. • You immediately delete any inappropriate message, image, photograph, animation, movie or drawing, which you may receive from outside Yubi. You do not forward this type of material. • You immediately notify a manager if you should receive an inappropriate message, image, photograph, animation, movie or drawing from an individual within Yubi. • You do not open unexpected email attachments. • You do not synchronize or connect in any way personal mobile phones or Personal Digital Assistants (PDAs) with any Yubi owned computer or mobile phone. • You do not publish your Yubi email address on the Internet, for example, in news groups or on public discussion boards. |
| Personal Liability | <ul style="list-style-type: none"> • If you do decide to use Yubi computer systems for personal purposes, you do this on the understanding that you accept full responsibility and liability for any purchases, transactions and actions. Yubi shall bear no responsibility for any damages whatsoever for any reason. |

7. Monitoring and Compliance

| | |
|--|---|
| Yubi Security Systems | <ul style="list-style-type: none"> • Yubi has installed a variety of security systems to assure the safety and security of the company networks. Any employee who attempts to disable, defeat or circumnavigate any company security facility will be subject to disciplinary procedures. |
| Instructions from IT Service Centre | <ul style="list-style-type: none"> • From time to time, you will receive instructions from the IT team, for example, asking you to switch off your workstation, scan your machine for virus, etc. These instructions must be followed and failure to do so will be considered as a breach of this agreement. |

| | |
|--|---|
| Audits, Monitoring & Investigations | <ul style="list-style-type: none"> Company computer systems, including Internet and email use will be subject to audits, monitoring, inspections and investigations and consequently you cannot expect any right of privacy when using them. Yubi reserves the right to monitor and record all computer use including Internet and email use. Monitoring uses automated processes for the purposes of identifying malpractice, protecting the company and individuals and complying with legal requirements. Monitoring is intended to identify activities such as, but not limited to, fraud, disclosure of confidential information, prevention of access to pornography and other malpractices. We respect individual privacy and due care will be taken not to invade it, unless authorized by management. Please note that only authorized personnel have access to the monitoring mechanism. |
| Acknowledgment of Yubi Rights | <ul style="list-style-type: none"> By using the computer systems, you acknowledge the right of Yubi to examine your user accounts for malpractice and, if necessary, to pass on data to a third party for investigation. |
| Disciplinary Action | <ul style="list-style-type: none"> Failure to adhere to organization's policies could lead to formal disciplinary action being taken and may result in dismissal. |
| Requests from Law Enforcement | <ul style="list-style-type: none"> Yubi will comply with legitimate requests from law enforcement and regulatory agencies for logs, diaries and archives on individuals' activities. INFORMATION TECHNOLOGY ACT, 2000 COPYRIGHT ACT, 1957 Amendment 2017. |

8. Protecting Information

| | |
|--|--|
| Protection of Company Sensitive and Personnel Information | <ul style="list-style-type: none"> You are required to protect the confidentiality of sensitive information, including information about people, and need to recognize that email is not secure, especially when sent outside Yubi. When using a computer in a public place, you should not access sensitive information and ensure that your screen cannot be overlooked. |
| Auto-Forwarding of Email | <ul style="list-style-type: none"> The auto-forwarding of email to a home or other external computer is not permitted. Sensitive information must not be forwarded outside of the company. |
| Handling of Printouts | <ul style="list-style-type: none"> Printouts from computers containing sensitive information must be handled and disposed of in a secure manner. |
| Processing of Personal Data | <ul style="list-style-type: none"> Unless it is integral to your role, you may not collect or process data about people without approval from your manager. |

| | |
|---|--|
| Maintaining Confidentiality of Private Information | <ul style="list-style-type: none"> Information of private nature regarding the Company and the company's clients is referred to as Private information. This may include business, strategies, methodologies, operations, technologies (including computer software, source code), financial affairs, organizational and personnel matters, policies, procedures, trade secrets, programs, operations, clients, prospective clients, employees and other non-public matters, including those concerning third parties. An employee will not during the period of his employment by the Company nor at any time thereafter, directly or indirectly, disclose or copy or distribute and/or use for his own benefit or for the benefit of others, Private Information acquired by him during the period of his employment. Every employee must maintain and assist the Company in maintaining the confidentiality of all Private Information and prevent it from coming into unauthorized hands. |
|---|--|

9. Work from Home Policy

| | |
|----------------------------------|--|
| Work from Home Guidelines | <ul style="list-style-type: none"> Employees when allowed to work remotely are expected to follow the same obligations as in working from the office. If, while working from a designated workspace, the employee experiences technical issues with his or her computer or internet access that prevent the employee from working remotely, the employee must notify his or her manager immediately. The assets provided by the company should be securely handled and not to be used for personal use. Employees login using the secured VPN provided by the company. Employees working from a remote workspace will be expected to attend all essential meetings via video conference or by phone only using authorized meeting tools/applications. Employees follow the regular working hours unless otherwise specifically mentioned based on the project requirements. Employees working from a remote workspace understand that the office desktop/mobile devices and their connectivity to the corporate network is being monitored by the Company periodically. Employees working remotely are reminded that even if they are working from a designated workspace, they are bound by any confidentiality and/or security agreements they signed in connection with their employment with Yubi and any confidentiality and/or security policies contained in Yubi Employee Handbook. |
|----------------------------------|--|

10. Security Reporting

| | |
|----------------------------|---|
| Security Problems | <ul style="list-style-type: none"> You are required to inform your manager or ISMS team or IT team if you become aware of any security problem, incident of suspected abuse or material that you believe contravenes this agreement and to retain any evidence. Report all information security incidents to infosec@yubi.com or call IT team on +91-4440074800 |
| Unauthorized Access | <ul style="list-style-type: none"> You should notify your manager at once if you have reason to believe that someone has obtained unauthorized access to systems by using your account. |
| Computer Viruses | <ul style="list-style-type: none"> If you suspect the presence of a computer virus, you are required to report it immediately to the IT team. |

11. Additional Privileges


| | |
|---|--|
| Additional Access Privileges | <ul style="list-style-type: none"> You may be issued with computer equipment or given additional access privileges that require you to follow additional regulations and procedures. Additional privileges issued for test and development environments must only be used for the purposes agreed. Non-compliance may result in disciplinary action. |
| Retention of Additional Privileges | <ul style="list-style-type: none"> If you are issued with additional privileges for your role, these privileges must only be used for the purpose agreed and you must ensure that these rights are removed if your role changes. |

12. Reporting of Security Incidents

| | |
|------------------------|---|
| Contact Numbers | <p>Email: infosec@go-yubi.com</p> <p>IT Members at IT.Team@go-yubi.com</p> |
|------------------------|---|

Agreed and accepted by:

Employee Name : Harish B

Signature : 

Harish Baskaran (February 27, 2023, 9:27 GMT)

Date : 27-Feb-2023

ISMS Document

Information Security Policy

Document Control ID: Yubi-ISP-10

Issued Date: 19-10-22

Published Date: 19-10-22

Confidential and Proprietary Information of CredAvenue Private Limited ('Yubi'). Only expressly authorized for individuals under obligations of confidentiality with Yubi are permitted to review materials in this document. By reviewing these materials, you agree to not disclose these materials to any third party unless expressly authorized by CredAvenue Private Limited and to protect the materials as confidential and trade secret information. Any unauthorized review, retransmission, dissemination, or other use of these materials is strictly prohibited. If you are not authorized to review these materials, please return these materials (and any copies) from where they were obtained. All materials found herein are provided "AS IS" and without warranty of any kind.

DOCUMENT AND RECORD CONTROL

Revision Table

| Date | Version | Brief Description | Author |
|-----------------|---------|-------------------------------------|--------------------|
| 01-August-21 | 0.1 | Information Security Policy – Draft | Abinesh Athilingam |
| 29-September-21 | 1.0 | Information Security Policy | Abinesh Athilingam |
| 26-September-22 | 1.1 | Formatting changes | Devika Subbaiah |

Approval History

| Date | Version | Approval | Title |
|-----------------|---------|----------|-------------------------|
| 29-September-21 | 1.0 | Approved | Chief Executive Officer |
| 19-October-22 | 1.1 | Approved | CISO |

Important Note: This document is intended solely for the use of the individual or entity to whom it is transmitted to, and others authorized to receive it. It may contain confidential or legally privileged information. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this document is strictly prohibited and may be unlawful. If you have received this document in error, please notify us immediately.

TABLE OF CONTENTS

| | |
|---|-----------|
| Office of Responsibility | 4 |
| Purpose | 4 |
| Scope | 4 |
| Management Commitment | 4 |
| Information Security Education and Awareness | 4 |
| Acceptable Use | 5 |
| Data Classification | 5 |
| Information Handling | 5 |
| Asset Management | 5 |
| Identity and Access Management | 5 |
| Database Security | 6 |
| Encryption | 6 |
| Secure Development | 7 |
| Cloud Security | 7 |
| Physical Security | 7 |
| Software Usage and Virus Protection | 8 |
| Security Logging and Monitoring | 8 |
| Incident Management | 8 |
| Vulnerability and Patch Management | 9 |
| Risk Management | 9 |
| Mobile Communications | 9 |
| Clean Desk & Clear Screen | 9 |
| Messaging Security | 9 |
| Remote & Mobile Computing | 10 |
| Roles and Responsibilities | 10 |
| Policy Enforcement and Compliance | 11 |

| | |
|---|-----------|
| Waiver Criteria | 12 |
| ISO 27001 References | 12 |
| Related Policies | 12 |
| Document Management | 13 |
| Appendix A: General Disclosure Statement | 13 |

1. Office of Responsibility

Chief Information Security Officer

2. Purpose

The Policy is aligned to the Information Security Program Charter which adheres to the risk management approach for developing and implementing Information Security Policies, standards, guidelines, and procedures. The policy defines the company's approach to managing information security and information systems protection and communicates the responsibilities that all employees have for maintaining information security program across the company.

3. Scope

The policy applies to all individuals who access, use or control CredAvenue Private Limited ('Yubi'), Yubi Securities Private Limited and its subsidiaries (hereinafter collectively referred to as "Yubi") owned resources. This includes but is not limited to Yubi's employees, third parties (contractors, consultants and other workers including all personnel affiliated to external organizations), investors, customers, other internal and external stakeholders with access to the Yubi's resources, network.

The Policy does not cover issues related to general physical and building security. It covers, however, physical security aspects of buildings or parts of buildings that directly affect the security of information owned by Yubi.

4. Management Commitment

Yubi is committed to preserving the security of all assets (including information) owned by and entrusted to it and ensuring the Security and Legal conformity. Yubi Management understands their responsibilities toward sustaining the information security objectives within the environment. Yubi Management acknowledges the importance of ensuring information security and is committed towards supporting the information security goals and its principles.

Yubi Management shall establish information security objectives aligned to its business objectives, information security requirements and pertaining risks. Shall develop detailed plans to measure, communicate, update, and achieve information security objectives. Yubi shall meet all applicable legal and/or regulatory requirements pertaining to information management.

5. Information Security Education and Awareness

Employees must acknowledge and adhere to the Yubi's Information Security Policy and any revisions to the policy and other related policies as instructed by Management.

Management shall establish a program to disseminate information security training to employees upon hiring and on a periodic basis. Appropriate training material should be developed based upon job function, and additional training mandated for roles with information security responsibilities.

6. Acceptable Use

The purpose of Yubi's Acceptable Use Policy is to establish the acceptable use of information systems at Yubi to ensure these systems are to be used only for business purposes in serving the interests of the company, and our clients and customers during normal operations. Inappropriate use exposes Yubi to risks including virus attacks, legal issues, and a compromise of network systems and services. Please review Yubi's Employee Handbook for further details.

7. Data Classification

The classification of all data received, processed, produced, and stored by Yubi and its member companies is vital in determining what baseline processes and mechanisms are appropriate for safeguarding that data.

Data shall be classified as to its sensitivity to the organization and security controls shall be applied accordingly. Data shall be labelled and handled in line with its classification. Data Owners or their assigned delegates should evaluate and assign appropriate classification based on the value and sensitivity of the information in accordance with the Information Classification, Labelling and Handling Policy.

8. Information Handling

Yubi's Information Classification, Labelling and Handling Policy defines the fundamental principles for the protection of Personal Data that is collected, obtained, used, maintained, accessed, transferred, transmitted, stored, disclosed, destroyed, or otherwise processed during the course and after the conclusion of the user's employment with Yubi. Yubi is committed to ensuring the privacy of employee data by using it only for legitimate business purposes, treating such data confidentially, and safeguarding it in accordance with Yubi's Information Classification, Labelling and Handling Policy.

9. Asset Management

All Yubi Information Assets shall be clearly identified, documented, and regularly updated in a Configuration Management Database (CMDB) or an asset inventory. All such assets shall have designated business, data, application, and system owners. All Yubi employees shall use company assets in accordance with the Yubi's Acceptable Use Policy and be classified in accordance with Yubi's Information Classification, Labelling and Handling Policy. Yubi's Asset Management Policy pertains to all Yubi's Information Assets, including but not limited to hardware and software, products and services, applications, servers, workstations, mobile devices, networking devices, firewalls, phones, printers, facsimiles and cabling. This includes assets managed on premises as well as those supported by third-party hosting and cloud-based services.

10. Identity and Access Management

Each employee shall be responsible for the actions completed by their user account. Yubi users must keep their user accounts and passwords confidential; shared or group user accounts are not permitted. If a user believes that their user account information may no longer be confidential, they must report it to the IT Help Desk immediately.

Information access shall be defined by a principle of least privilege and access rights shall be limited to the minimum necessary to perform job functions. All employees shall be authorized according to guidelines defined by Business Owners and Data Owners, in cooperation with the

Information Security in creation of appropriate rules and role-based access controls.

- All computers must be protected by approved password-based access control systems.
- Multi-factor authentication for remote access to corporate and production networks by employees, administrators, and third parties shall be implemented where applicable.
- Details for access control processes and standards, as well as password control, reset and complexity requirements are found in the Access Management Policy.

11. Database Security

Define and implement procedures to ensure the integrity and consistency of all information stored

in electronic form such as databases, data warehouses and data archives. Sensitive data must be protected in accordance with the Yubi Information Classification, Labelling & Handling Policy. Data subject to encryption must adhere to the Yubi Encryption Policy.

Data owners, application owners, system owners, product owners, and all others involved in the system lifecycle must always know and fully document the location of all data – especially Protected Regulated Information. Documentation must be updated continually. Database accounts used by DBAs for administrative duties must be unique individual accounts, and not shared group accounts. Activities performed by these accounts must be effectively monitored by independent personnel.

All multi-user, business critical or restricted databases must be inventoried at the appropriate level. Additionally, some description of database contents is required; detailed descriptions will be required when the database contains Protected Regulated Information (see Information Classification, Labelling and Handling Policy).

Servers and host systems on database and application hosts must be configured and administered according to the Hardening Standards. This includes all changes to configuration, and any changes to the location of Protected Regulated Information. The database software version must be currently supported by the vendor.

12. Encryption

Encryption shall be used, where required, either contractually or by the Information Classification, Labelling and Handling Policy, to protect the confidentiality, authenticity and/or integrity of information. Management shall implement cryptographic measures that are consistent with regulatory requirements for protected information. Details for the specific principles related to encryption are found in the Encryption and Key Management Policy.

PKI shall be used for enabling trusted communications. Usually, PKI contains a high-level Application Program Interface (API) that handles tasks such as verifying and managing certificates, digitally signing documents, and managing keys. The API serves as a layer between application programs like secure e-mail and the underlying security services. The API allows applications to reliably use public key cryptography for security without being concerned about the details of its implementation.

13. Secure Development

Information security requirements shall form an integral part of systems development lifecycle, including requirements for information systems that provide services over public networks i.e., the internet. System development shall follow processes to ensure secure coding practices, application vulnerability scanning, and formal change control procedures that address documentation, approval, testing and implementation of changes.

Systems in development and/or testing environments shall be segmented from production networks and information systems. Access to these segmented networks and development systems shall be limited to approved personnel only.

Public Key Infrastructure (PKI) for authentication shall be utilized for all verification of authentication within the software.

14. Cloud Security

The Scope statement of this Framework indicates that information that is physical, electronic, and processed and stored either by Yubi's managed processing facilities or vendor and cloud-based service providers must adhere to Yubi's Information Security Policies. The Policy mandates that for cloud services to be deployed, specific approval of Yubi's business, finance and technology

must be obtained. It is imperative that Yubi employees do not open cloud services accounts or enter cloud service contracts for the storage, manipulation or exchange of company-related communications or company-owned data without the approval of the Information Security Head/Business head. The policy pertains to all external cloud services, e.g., cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc.

15. Physical Security

All Yubi facilities and information resources, including all protected areas, shall have appropriate physical access controls in place to protect them from unauthorized access. Other protective measures, such as video surveillance of physical information resources and systems, as well as safeguards against environmental hazards and electronic penetration, shall be maintained.

All computing and electronic devices, such as desktop computers, must be accompanied by an authorization from the data owners when it is being removed from a Yubi location.

To prevent loss, damage, theft or compromise of Yubi computer assets, physical media, and confidential documents, and mobile devices, shall be handled in accordance with the Physical Security Policy.

16. Software Usage and Virus Protection

Software installed on any machine connecting to a Yubi or member company network must only be used for business purposes. Employees are prohibited from using any unlicensed software as well as freeware, streaming (i.e., stock ticker, news services, etc.), or peer-to-peer software without the consent of Yubi's VP of Information Security and Compliance and the respective Business Owner. Only authorized, supported, and properly licensed software shall only be installed on Yubi owned or managed systems.

Only IT administrators or specific personnel approved by Information Security who have been granted administrator access shall install authorized and licensed software. The use of unauthorized software is prohibited. Immediate removal of unauthorized software is required if discovered.

A security review and approval of all software shall be completed prior to production release. The review shall be based on system criticality and data type. Free, shareware, and open-source software as well as software as a service (SaaS) shall be reviewed as well.

Software that is end-of-life and no longer supported is considered unauthorized software and shall be subjected for Information security review before continuing to use.

Antivirus software must be installed on all Yubi workstations. Employees shall be prohibited from disabling antivirus software and employees must report malware incidents to the Information Security Incident Response Team for proper handling of potential or suspected viruses. The Information Security Team is responsible for triage and remediation of malware incidents, per the Information Security and Incident Management Procedure.

17. Security Logging and Monitoring

Yubi will monitor and maintain logs recording user activities, exceptions, faults and security events to allow for the detection and prevention of information security events. Logs shall be kept for sufficient time to support investigation of suspicious events and logs shall be regularly reviewed, in accordance with Cyber Security policy and regulatory requirements.

Logging software, tools, facilities and log information shall be protected against tampering and

unauthorized access. The system clocks of information processing systems shall be synchronized to an authoritative single time source to allow logs timestamps to be correlated.

18. Incident Management

The Information Security Organization shall implement processes and controls that monitor, identify, respond to, and remediate incidents that threaten Yubi information systems, services and supporting processes. An information security incident is defined as any event or activity that threatens the confidentiality, integrity and availability of Yubi information systems. An information security event is defined as any measurable occurrence out of the norm. It is the responsibility of all individuals to formally report information security events and incidents.

19. Vulnerability and Patch Management

Technical vulnerabilities for all information systems being used shall be monitored to ensure that the organization's exposure to such vulnerabilities is evaluated and appropriate measures taken to address the associated risk in a timely manner in accordance with the Vulnerability and Patch Management requirements in Cyber Security Policy.

A standard procedure and system shall be deployed for the monitoring and controlled deployment of system patches and updates according to a defined software lifecycle. A change control process should be documented to accurately account for software configuration control and monitoring.

20. Risk Management

Risk assessments shall be completed annually, in accordance with the development lifecycle method. Risk assessments shall also be completed upon major changes to the Yubi organization or infrastructure environment. The results of the assessment must be communicated to the business, and a summary of all risk acceptances or mitigations achieved must be documented.

21. Mobile Communications

All mobile devices connecting to Yubi resources are subject to the restrictions defined by organization. WiFi hotspot functionality, as found on various Android, Apple iOS, and other mobile devices, as well as 4G/5G mobile WiFi devices, are prohibited in Yubi office spaces unless express approval is obtained from the Information Security team. Theft or loss of a company mobile asset is considered an information security incident.

Remotely accessible Yubi information assets, including but not limited to web-accessible resources and file sharing systems, must be secured with encryption and authentication consistent with the framework in Yubi's Access Management Policy document.

22. Clean Desk & Clear Screen

The purpose for the policy is to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use, or a user leaves his/her workstation. The policy establishes the minimum requirements for maintaining a "clean desk" – where sensitive/confidential information about our employees, our intellectual property, our customers, and our vendors, as defined in Yubi's Information Classification, Labelling and Handling Policy, is secure in locked areas and out of site. Clean Desk Policy is a standard practice as per various frameworks such as NIST 800-53, SANS Top 20, ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

23. Messaging Security

All incoming emails shall be scanned for viruses, malwares and attempts for phishing will be

checked before delivering the emails to users' inbox.

All outgoing emails shall be verified with the data loss prevention (DLP) solution.

Any messaging service shall be approved by Information Security prior to usage and shall include appropriate audit trails and encryption of data at rest and in transit. Data loss prevention (DLP) tools and processes shall be implemented, where possible.

24. Remote & Mobile Computing

Appropriate controls shall be put in place to protect sensitive organization data on mobile and remote computing environments. Company data on employee-owned devices shall be removed within the timelines defined in HR policy.

Use of personally owned devices shall comply with acceptable use and cyber security policy if used to access personally identifiable information or any sensitive data.

Devices owned by personnel shall never be used to access company/customer data, unless appropriate security controls approved by information security are implemented. Also, these devices are not allowed to connect to the company or production network.

25. Roles and Responsibilities

Each role involved in the policy shall have main responsibilities as follows:

The Vice President of Information Security & Compliance

- Managing and implementing the policy and related policies, standards, and guidelines.
- Monitoring and responding to potential and/or actual IT security breaches.
- Ensuring that staff are aware of their responsibilities and accountability for information security.
- Act as a consulting contact for all security related issues.
- Act as a central point of contact on Information Security for both staff and external organizations.
- Acts as an approval authority for the Information Security policy and its exceptions.
- Review and signoff changes to Information Security policies prior submitting for approval from IS head.
- Responsible for information risk within Yubi advising the executive management on the effectiveness of management of security and privacy issues across the organization and advising on compliance with relevant legislation and regulations.
- Responsible for cascading and ensuring the implementation, operation, monitoring, maintenance, and improvement of the Integrated management system.

Managers

- Ensuring that the Information Security policy and associated standards and guidelines are properly communicated and understood within their respective organizational units.
- Defining, approving, and implementing procedures in their organizational units and ensuring their consistency with the Information Security Policy and associated standards and guidelines.
- Determining the level of access to be granted to specific individuals.
- Ensuring staff have appropriate training for the systems they use.
- Ensuring staff know how to access advice on information security matters.

All Employees

All individuals, groups, or organizations identified in the scope of the policy are responsible for familiarizing themselves and complying with the Information Security Policy and associated standards and procedures.

All employees are responsible for information security and therefore must understand and comply with the policy and associated guidance. Failure to do so may result in disciplinary action.

All employees should understand:

- What information they are using, how it should be used, stored, and transferred in terms of data security
- What procedures, standards and protocols exist for the sharing of information with other parties
- How to report a suspected breach of information security within the organization
- Their responsibility for raising any information security concerns.

All individuals are responsible with adhering to the provisions of the Policy and all related policies, standards, guidelines, and procedures and must report every incident of misuse or abuse of which they become aware as described in the policy.

26. Policy Enforcement and Compliance

Yubi recognizes its burden to exercise due care for the safeguarding of data in its custody including, but not limited to, Personally Identifiable Information (PII), Financial information and Yubi Intellectual Property. To this end, and for overall assurance of the confidentiality, integrity, and availability of Yubi information systems, an independent review of compliance with the Policy shall be conducted on a regular basis.

Yubi must adhere to applicable Reserve Bank of India's (RBI) Master directions for Non-Banking Financial Companies and RBI's IT Framework. This is not intended to be an exhaustive list of applicable regulatory requirements with respect to state or local laws that must similarly be complied with.

Further, all employees shall comply with relevant national and local legal, regulatory, and contractual requirements. Any Yubi employee who does not comply with the policy may be subject

to disciplinary action, up to and including termination. Access to Yubi information systems and resources is a privilege, not a right, and may be revoked or suspended at any time.

27. Waiver Criteria

The policy is intended to address information security requirements. If needed, waivers shall be formally submitted to the Information Security Management, including justification and benefits attributed to the waiver by the CISO.

The policy waiver shall be granted for a period of four months initially and shall be reassessed thereafter and can be extended up to a period of three consecutive terms. No waiver shall be provided for more than three consecutive terms on any of the policies.

28. ISO 27001 References

- A. 5.1.1 Policies for Information Security
- A. 5.1.2 Review of the Policies for Information Security
- Clause 5.1 Leadership and commitment
- Clause 5.2 Policy

29. Related Policies

- Acceptable Use Policy
- Clear Desk and Clear Screen Procedure
- Access Control Policy
- Asset Management Policy
- Backup Policy
- Legal and Regulatory requirement Procedure
- Encryption and Key Management Policy
- Human Resource Security Policy
- Business Continuity Management Policy
- Incident Management Procedure
- Risk Management Policy
- Secure Development LifeCycle Procedure

30. Document Management

Technological advances and changes in the business requirements will necessitate periodic revisions to documents. Therefore, this document may be updated to reflect changes or define new or improved requirements as and when required and in compliance with the Information Security Program Charter.

31. Appendix A: General Disclosure Statement


Unless specifically stated otherwise, all programs, data and documentation received, developed, stored and/or transmitted by employees are the property of Yubi. Yubi reserves the right to examine all information received, stored and/or transmitted by Yubi or its member companies' systems

including but not limited to email and Internet activity.

- Employees should have no expectation of privacy about the access or use of these systems, data or resources. Wilful or intentional misuse of Yubi or its member companies' systems and data can result in termination of access privileges as well as disciplinary action. In addition, this Information Security Policy reinforces the Yubi Employee handbook.
- All information belonging to Yubi and/or third parties deemed private, confidential, sensitive, or proprietary (Refer to Asset Identification and Classification Policy) which includes but is not limited to, Personally Identifiable Information (PII) or financial information, must be treated as such unless expressly authorized by Yubi Management, the Data Custodian, a disclosing party or by Law.
- Employees must use reasonable and prudent measures to protect all data from accidental or intentional damage, modification, destruction, or unauthorized disclosure. Moreover, Employees must ensure data integrity, reliability, and availability in accordance with this Information Security Policy, the Yubi Information Security Best Practice document, signed contractual agreements, and local, state, and national laws.
- Prior to or immediately upon separation of employment, all data in the possession of the Employee must be returned intact and without compromise according to any policies contained herein, expressed, or implied. Upon receipt, this information will be handled or stored in accordance with the policies contained in this document.
- Changes, questions or concerns regarding this Information Security Policy, should be directed to Yubi's VP of Information Security & Compliance by email.

I hereby agree and accept the policy.

Employee Name : Harish B

Signature : 

Harish Baskaran (February 27, 2023, 9:27 GMT)

Date : 27-Feb-2023

ISMS Document

Data Protection and Security Policy

Document Control ID: Yubi-ISP-12

Issued Date: 19-10-22

Published Date: 19-10-22

Confidential and Proprietary Information of CredAvenue Private Limited ('Yubi'). Only expressly authorized for individuals under obligations of confidentiality with Yubi are permitted to review materials in this document. By reviewing these materials, you agree to not disclose these materials to any third party unless expressly authorized by CredAvenue Private Limited and to protect the materials as confidential and trade secret information. Any unauthorized review, retransmission, dissemination, or other use of these materials is strictly prohibited. If you are not authorized to review these materials, please return these materials (and any copies) from where they were obtained. All materials found herein are provided "AS IS" and without warranty of any kind.

DOCUMENT AND RECORD CONTROL

Revision Table

| Date | Version | Brief Description | Author |
|-----------------|---------|---|--|
| 20-September-21 | 0.1 | Data Protection and Security Policy – Draft | Xavier Parakkal and Araveinth Gopinath |
| 29-September-21 | 1.0 | Data Protection and Security Policy | Xavier Parakkal and Araveinth Gopinath |
| 02-September-22 | 1.1 | Formatting changes | Devika Subbaiah |

Approval History

| Date | Version | Approval | Title |
|-----------------|---------|----------|-------------------------|
| 29-September-21 | 1.0 | Approved | Chief Executive Officer |
| 19-October-22 | 1.1 | Approved | CISO |

Important Note: This document is intended solely for the use of the individual or entity to whom it is transmitted to, and others authorized to receive it. It may contain confidential or legally privileged information. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this document is strictly prohibited and may be unlawful. If you have received this document in error, please notify us immediately.

TABLE OF CONTENTS

| | |
|---|-----------|
| Office of Responsibility | 3 |
| Purpose | 3 |
| Scope | 3 |
| Accountability | 3 |
| Policy | 4 |
| Personal Data Processing Principles | 4 |
| Fair & Lawful Processing | 4 |
| Legal Basis Customer Data | 4 |
| Legal Basis Employee Data | 5 |
| Processing of Highly Sensitive Data | 6 |
| Duty of Information/Transparency | 7 |
| Purpose Limitation | 7 |
| Data Minimization | 7 |
| Accuracy of Data | 7 |
| Privacy by Design | 7 |
| Data Anonymization and Deletion | 8 |
| Data Security: Processing | 8 |
| Data Transmission Outside of Company | 8 |
| Data Protection Impact Assessment | 9 |
| Records of Processing Activities | 9 |
| Processing in Line with Data Subject's Rights | 9 |
| Disclosure and Sharing of Personal Information | 10 |
| Reporting Breaches | 11 |
| Data Protection Organization Structure & Sanctions | 11 |
| Responsibility | 11 |

| | |
|---------------------------|-----------|
| Organization | 11 |
| Sanctions | 12 |
| Audit and Controls | 12 |

1. Office of Responsibility

The Chief Information Security Officer (“**CISO**”) & the Data Protection Officer (“**DPO**”).

2. Purpose

As stated in Yubi’s Information Security Program Charter (“**Information Security Program**”), CredAvenue Private Limited (‘Yubi’), Yubi Securities Private Limited and its subsidiaries (hereinafter collectively referred to as “**Company**”) will follow a risk management approach in developing and implementing Information Security policies, standards, guidelines, and procedures. The Information Security Program is designed to protect information assets by developing Information Security policies to identify, classify, and define the acceptable use of Company’s information assets.

This Data Protection and Security Policy (“**Policy**”) defines Company’s objectives for establishing specific standards on the protection of confidentiality, integrity, and availability of Company’s information assets. The Policy provides adequate guarantees for the protection of personal data of the organization and its customers.

3. Scope

The Policy applies to all employees, contractors, consultants, and vendors.

The Policy applies to fully or partially automated processing of personal data, as well as manual processing in filing systems unless applicable laws provide for a broader scope. The Policy also applies to all employee data kept/preserved in paper/ magnetic/ optical media.

The Policy applies to all subsidiaries of the Company operating within its scope of application.

4. Accountability

- The Company shall use its best efforts to integrate data protection policies set out herein into any new technology planning or processing activities undertaken by it.
- The DPO is responsible for ensuring compliance with the data protection regulation and with the Policy. Any questions about the operation of the Policy or any concerns that the Policy has not been followed should be referred in the first instance to the DPO.
- The DPO is an independent officer, appointed to carry out the following tasks.
 - Inform and advise Company and its subsidiaries or our data processors who carry out processing activities of their obligations under the data protection regulations and the Policy.
 - Monitor our compliance with applicable privacy and data protection legislation and the Policy.
 - Provide advice where requested with regards to the data protection impact assessment and monitor its performance.
 - Act as the point of contact and co-ordinate with the judicial, quasi-judicial or governmental authorities to find a speedy resolution to issues raised in relation to any processing of data.

- Data Subjects may contact the DPO with regards to all issues related to processing of their personal data and in respect of their rights under the data protection laws.
- The Company shall ensure all its directors, officers, employees, and agents comply with the policy and to this effect, conduct appropriate training for them.
- In order to enhance the integrity and independence of the DPO, the office of DPO reports directly and only to the respective Company's executive management team.

5. Policy

5.1 Personal Data Processing Principles

5.1.1 Fair & Lawful Processing

Personal data shall be processed in good faith and in a lawful manner for the purpose it is collected. Data processing may only take place if and in so far as a sufficient legal basis exists for the processing activity. The processing of personal data is lawful if one of the following circumstances for authorization under paragraphs 5.1.2 or 5.1.3 of the Policy applies. Such circumstances for permissibility are also required if the purpose of processing the personal data is to be changed from the original purpose.

5.1.2 Legal Basis Customer Data

Data Processing for Contractual Relationship

Personal data of the prospective customer, customer, or partner can be processed, to establish, perform and terminate an agreement or a contract, pursuant to the respective individual's consent obtained as per the applicable laws in force at the time, to establish, perform and terminate a contract. This may also include advisory services for the customer or partner under the contract, if this is related to the contractual purpose.

Prior to a contract, personal data can be processed to prepare bids or purchase orders or to fulfil other requests of the prospective customer relating to contract conclusion. Prospective customers can be contacted during the contract preparation, negotiation, finalization or execution process using the information that they have provided. Any restrictions requested by the prospective customers must be complied with.

Consent to Data Processing

Personal data can be processed following the consent by the data subject. Before giving consent, the data subject must be informed in accordance with the Policy. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In some circumstances, such as telephone conversations, consent can also be given verbally. The granting of consent must be documented.

Data Processing Pursuant to Legal Authorization or Obligation

The Company may, at the instruction, or order of the judicial, quasi-judicial or governmental authorities, process data in accordance with the applicable laws in force at the time of such instruction. The nature, scope and extent of personal data and its processing will be determined by the judicial, quasi-judicial or governmental authorities and the applicable laws in force.

Data Processing Pursuant to Legitimate Interest

Personal data can also be processed if it is necessary for a legitimate interest. Legitimate interests are generally of a legal (e.g., collection of outstanding receivables) or commercial nature (e.g., avoiding breaches of contract). Processing cannot take place on the basis of a legitimate interest if, in a specific instance, the data subjects' interests worthy of protection outweigh the legitimate interests in processing. Before data is processed, it is necessary to determine whether there are interests worthy of protection.

5.1.3 Legal Basis Employee Data

Data Processing for the Employment Relationship

For employment relationships, personal data can be processed if needed to establish, perform, and terminate the employment relationship. Personal data of candidates can be processed to complete background checks prior to entering into an employment relationship. If the candidate is rejected, his/ her data must be deleted in observance of the required retention period, unless the candidate has agreed to remain on file for a future selection process. Consent is also needed to use the data for further application processes or before sharing the application with subsidiaries of the Company.

In the existing employment relationship, data processing must always relate to the purpose of the employment relationship if none of the following circumstances for authorized data processing apply. If it should be necessary during the application procedure to collect information on an applicant from a third party, the requirements of the corresponding data protection laws have to be observed. In cases of doubt – where permitted – consent must be obtained from the data subject.

A legal basis as listed below must be met to process personal data that is related to the employment relationship but was not originally part of creating, performing or terminating the employment relationship (employee data).

Data Processing Pursuant to Legal Authorization or Obligation

The processing of employee data is also permitted: (i) based on employee's consent; (ii) for the performance of the employment agreement; (iii) at the instruction, or order of the judicial, quasi-judicial or governmental authorities, process data in accordance with the applicable laws in force at the time of such instruction; or (iv) for legitimate interest. The nature, scope and extent of personal data and its processing will be determined by the applicable laws in force and the judicial, quasi-judicial or governmental authorities (if processed pursuant to instructions of the judicial, quasi-judicial or governmental authorities).

Collective Agreement on Data Processing

If a data processing activity exceeds the purposes of fulfilling a contract and those set out in paragraph 5.1.3.2, it may still be lawful if authorized through a collective agreement. The agreements must cover the specific purpose of the intended data processing activity and must be drawn up within the parameters of data protection requirements outlined by regulatory or Government of India.

Consent to Data Processing

Employee data can be processed upon consent of the data subject. Declarations of consent must be submitted voluntarily. No penalties can be imposed for refusal of consent. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. If exceptional circumstances do not permit this, consent may be given

verbally. In any case, such verbal consent must be properly documented. Before giving consent, the data subject must be informed in accordance with this Data Protection Policy.

Data Processing Pursuant to Legitimate Interest

Employee data can also be processed if it is necessary for a legitimate interest of the Company. Legitimate interests are generally of a legal (e.g., filing, enforcing, or defending against legal claims) or a commercial nature (e.g., acceleration of business processes, valuation of companies). Before data is processed, it must be determined whether there are interests worthy of protection. Personal data can be processed based on a legitimate interest if the interests worthy of protection of the employee do not outweigh the interest in processing.

Control measures that require the processing of employee data beyond performance of the employment relationship (e.g., performance checks) cannot be taken unless there is a legal obligation or justified reason to do so. Even if there is a legitimate reason, the proportionality of the control measure must also be examined. To this end, the legitimate interests of the Company in performing the control measure (e. g. compliance with legal provisions and internal company rules) must be weighed against any protective interests that the employee affected by the measure may have in exclusion of the measure. The measures may only be taken if they are appropriate in the specific case. The legitimate interest of the Company and any interests worthy of protection of the employee must be identified and documented before any measures are taken. Moreover, any additional requirements under applicable law (e.g., rights of co-determination for the employee representatives and rights of the data subjects to obtain information) must be taken into account.

5.1.4 Processing of Highly Sensitive Data

The processing of highly sensitive personal data must be expressly permitted or prescribed under the data protection regulation of India. Processing of such data by Company may be permitted in particular if the data subject has given his express consent, if the processing is necessary for asserting, exercising or defending legal claims with respect to the data subject or if processing is necessary for the controller to fulfil its rights and responsibilities in the area of labour and employment law. If there are plans to process highly sensitive personal data, the DPO must be informed in advance.

5.1.5 Duty of Information/Transparency

The responsible department must inform the data subjects of the purposes and circumstances of the processing of their personal data in a concise, transparent, intelligible and easily accessible form and in clear and plain language. The requirements of the DPO must be observed. This information must be given whenever the personal data is collected for the first time. If the Company receives the personal data from a third party, it must provide the information to the data subject within a reasonable period after obtaining the data, unless

- The data subject already has the information or
- It would be impossible or
- Extremely difficult to provide this information

5.1.6 Purpose Limitation

Personal data may be processed only for the legitimate purpose that was defined before

collection of the data or the purposes which are ancillary or essential for fulfilment of the purpose of collection of data. Subsequent changes to the purpose of processing are only permissible subject to the requirement that the processing is compatible with the purposes for which the personal data was originally collected.

5.1.7 Data Minimization

Any processing of personal data must be limited, both quantitatively and qualitatively, to what is necessary for the achievement of the purposes for which the data is lawfully processed. This must be taken into account during the initial data collection. If the purpose permits, and the effort is in proportion to the objective pursued, anonymized or statistical data must be used.

5.1.8 Accuracy of Data

The personal data stored must be objectively correct and, if necessary, up to date. Appropriate measures must be adopted to ensure that incorrect or incomplete data is deleted, corrected, supplemented or updated.

5.1.9 Privacy by Design

The principle of “Privacy by Design” aims to ensure that technology team define state-of-the-art internal strategies and adopt measures to integrate data protection principles into the specifications and architecture of business models/processes and IT systems for data processing from the very beginning during the phase of conceptualization and technical design. In accordance with the principle of “Privacy by Design,” the procedures and systems for processing personal data must be designed so that their default settings are restricted to the data processing necessary to fulfil the purpose. This includes the processing scope, storage period, and accessibility. Further measures could include:

- Pseudonymization of personal data as soon as possible
- Providing transparency about the functions and processing of personal data
- Allowing the data subjects to decide on the processing of their personal data
- Enabling the operators of procedures or systems to devise and enhance security features

The Company shall implement and maintain appropriate technical and organizational measures throughout the entire life cycle of its processing activities, in order to ensure that the above principles are complied with at all times.

5.1.10 Data Anonymization and Deletion

Personal data may only be stored for as long as it is necessary for the purpose for which the data is being processed. This means that personal data must be deleted or anonymized, in accordance with the regulations as soon as the purpose of its processing has been fulfilled or otherwise lapses, unless documentation or retention obligations continue to apply. Those responsible for individual procedures must ensure the implementation of the deletion and anonymization routines for their procedures.

Each system must have a manual or automated deletion routine. Deletion requests from data subjects through deletion or removal of the personal identifiers must be technically feasible in the systems. Requirements that Company imposes for the performance of deletion routines (such as software tools, handout for the implementation of deletion

concepts, documentation requirements) must be observed.

5.1.11 Data Security: Processing

Personal data must be protected from unauthorized access and unlawful processing or transfer, as well as from accidental loss, alteration or destruction. Before the introduction of new methods of data processing, particularly new IT systems, technical and organizational measures to protect personal data must be defined and implemented. These measures must be based on the state of the art, the risks of processing and the need to protect the data.

The technical and organizational measures relevant to data protection must be documented by the Company in the context of the Data Protection Impact Assessment and the Record of Processing Activities.

In particular, the responsible product owner must consult with its DPO. The requirements for the technical and organizational measures for protecting personal data are part of the Company's Information Security Management and must be continuously adjusted in accordance with technical developments and organizational changes.

5.1.12 Data Transmission Outside of Company

Transmission of personal data to recipients outside or inside the Company is subject to the authorization requirements for processing personal data under paragraph 5 of the Policy. The data recipient must use the required data only for defined purposes.

Transfers of personal data to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is permissible in law.

In the event of conflicts between these and public authority requirements, the Company will work with the responsible technology team to find a practical solution that fulfills the purpose of the Policy.

All duties listed in paragraph 5 of the Policy are third party beneficiary rights for the data subject.

5.2 Data Protection Impact Assessment

In the event new processing activities are introduced or we develop new technologies into our business, an assessment of the impact of the change in operations on the protection of such personal data shall be carried out in order to address any processing operations that present a high risk to the rights and freedoms of the data subjects or risk non-compliance with the data protection regulations.

Such assessment will be carried out with the advice of DPO.

As part of the risk analysis, the responsible product team carries out an assessment of the impact of the planned processing on the protection of personal data (Data Protection Impact Assessment). Provisions established by the Company for performing this assessment (such as software tools, instructions on the performance of an evaluation) must be observed. These instructions and tools are available in the internal wiki site.

5.3 Records of Processing Activities

Company shall maintain a record of processing activities which we carry out. The record shall contain the below information:

- The name and contact details of the data controller.
- Purpose of the processing.
- Description of the categories of data subjects and categories of personal data.
- The categories of recipients to whom the personal data have been or will be disclosed include recipients in third countries or international organisations and the documentation of suitable safeguards concerning this disclosure.
- Time limits of erasure of the different categories of data.

5.4 Processing in Line with Data Subject's Rights

- Company shall process all personal data in line with data subjects' rights, in particular their right, in certain circumstances, to:
 - Transmit their data to another data controller (free of charge), where such personal data is processed on the basis of consent or contractual performance, unless in doing so, it would adversely affect the rights or freedoms of other data subject's or others e.g., including trade secrets or intellectual property.
 - Prevent the processing of their data or withdraw their consent at any time in certain circumstances.
 - Ask to have inaccurate data amended.
 - Erasure of their personal data where data is no longer required for the original purpose or where the data subject has withdrawn their consent and no other lawful processing grounds apply.
 - Object to the processing of their personal data in certain circumstances.
 - Be notified where their personal data is subject to automated decision making i.e., profiling, including the logic involved, as well as the significance and the envisaged consequence of such processing for the data subject and object to such profiling in certain circumstances.
 - Invoke binding arbitration to resolve complaints not resolved by other means.
- Where we are required to provide a copy of personal data this will be free of charge, however, any further copies requested may be subject to reasonable fee based on administration costs.
- When we stop processing personal data or delete a data subject's personal data, it will possibly mean that the data subject is unable to continue using or contributing to the provision of some of our services, and they shall be notified accordingly.

- Where a data subject requests to rectify or erase their personal data or restrict any processing of such personal data, we may be required to notify certain third parties to whom such personal data has been disclosed of such request.

5.5 Disclosure and Sharing of Personal Information

- The Company may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries.
- We may also disclose personal data we hold to third parties.

If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

Disclosing/sharing personal data outside of our organisation carries further risks and we must ensure the right organisational, technical, and contractual measures are in place before transferring or allowing access to personal data.

5.6 Reporting Breaches

Where there has been a personal data breach and the breach is likely to result in a high risk to the rights and freedoms of the data subject, Company will report the breach to the regulatory authority (if required) without undue delay and, where feasible, not later than 72 hours after having become aware of it.

Complaints Procedure

Data subjects are entitled to file a complaint with the DPO if they feel that the Policy has been violated. Complaints of this kind can be submitted by e-mail to the DPO.

6. Data Protection Organization Structure & Sanctions

6.1 Responsibility

The members of managing bodies of the Company are responsible for data processing in their area of responsibility. Therefore, they are required to ensure that the legal requirements, and those contained in the Policy, for data protection are met. Within their area of responsibility, management staff is responsible for ensuring that organizational, HR and technical measures are in place so that any data processing is carried out in accordance with data protection requirements. Compliance with these requirements is the responsibility of the relevant employees. If public authorities perform data protection checks, the DPO must be informed immediately.

6.2 Organization

The DPO is internally independent of instructions regarding the performance of his tasks. He must ensure compliance with national and international data protection laws (as applicable). He is responsible for the Policy and monitors its compliance. The DPO is appointed by the Company's Board of Management. Generally, Company and subsidiaries that are legally obligated to appoint a DPO will appoint a DPO. Specific exceptions have to be agreed upon with the Yubi's DPO.

All data subjects can contact the DPO at any time to express their concerns, ask questions, request information or lodge complaints relating to data protection or data security issues. If requested, concerns and complaints will be handled confidentially.

The contact information of the DPO is:

Yubi,
Data Protection Officer (DPO),
Prestige polygon towers, No. 471,
Anna Salai, Nandanam, Chennai | 600035
E-Mail: data.protection@go-yubi.com

The Company has also established a compliance organization, which is described in greater detail in separate internal documents. It defines the content of the data protection training and stipulates the criteria for the group of participants.

6.3 Sanctions

Unlawful processing of personal data or other offences against data protection law can be prosecuted under regulatory and criminal law in many countries and can also lead to claims for compensation. Breaches for which individual employees are responsible can lead to disciplinary action under Human Resources policy. Violations of the Policy will be penalized in accordance with internal regulations.


6.4 Audit and Controls

Compliance with the Policy and the applicable data protection bill will be reviewed regularly at Company level (or group level) by way of data protection audits and other checks. The results of these audits must be reported to the DPO, the responsible Company and its DPO if one has been appointed. Moreover, the results of this audit must be provided to third-party controllers in accordance with the contractual provisions of the agreement on processing on behalf. The Company must also perform its own examinations and reviews to determine compliance with the Policy, if so, requested by the DPO.

The Company's Management & Board must be informed of significant findings as part of existing reporting duties. On request, the results of the reviews will be made available to the competent data protection supervisory authority (if any and as required). The competent data protection supervisory authority can perform its own checks on compliance with the regulations of the Policy.

I hereby agree and accept the policy.

Employee Name : Harish B

Signature : 

Harish Baskaran (February 27, 2023, 9:27 GMT)

Date : 27-Feb-2023

ISMS Document

Privacy Policy

Document Control ID: Yubi-ISP-13

Issued Date: 19-10-22

Published Date: 19-10-22

Confidential and Proprietary Information of CredAvenue Private Limited ('Yubi'). Only expressly authorized for individuals under obligations of confidentiality with Yubi are permitted to review materials in this document. By reviewing these materials, you agree to not disclose these materials to any third party unless expressly authorized by CredAvenue Private Limited and to protect the materials as confidential and trade secret information. Any unauthorized review, retransmission, dissemination, or other use of these materials is strictly prohibited. If you are not authorized to review these materials, please return these materials (and any copies) from where they were obtained. All materials found herein are provided "AS IS" and without warranty of any kind.

DOCUMENT AND RECORD CONTROL

Revision Table

| Date | Version | Brief Description | Author |
|-----------------|---------|------------------------|--------------------|
| 20-September-21 | 0.1 | Privacy Policy – Draft | Abinesh Athilingam |
| 29-September-21 | 1.0 | Privacy Policy | Abinesh Athilingam |

Approval History

| Date | Version | Approval | Title |
|-----------------|---------|----------|-------------------------|
| 29-September-21 | 1.0 | Approved | Chief Executive Officer |
| 19-October-22 | 1.1 | Approved | CISO |

Important Note: This document is intended solely for the use of the individual or entity to whom it is transmitted to, and others authorized to receive it. It may contain confidential or legally privileged information. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this document is strictly prohibited and may be unlawful. If you have received this document in error, please notify us immediately.

TABLE OF CONTENTS

| | |
|--|----------|
| Office of Responsibility | 3 |
| Purpose | 3 |
| Scope | 3 |
| Policy | 3 |
| Objectives | 3 |
| Policy Compliance | 6 |
| Responsibilities | 6 |
| Policy Enforcement and Compliance | 6 |
| Document Management | 6 |

1. Office of Responsibility

Chief Information Security Officer

2. Purpose

As stated in the Company Information Security Program Charter, the Company will follow a risk management approach to developing and implementing Information Security policies, standards, guidelines, and procedures. The Information Security Program is designed to protect information assets by developing Information Security policies to identify, classify, and define the acceptable use of company information assets.

The Privacy Policy defines Company objectives for securing and protecting personally identifiable information and other information.

The types of personal data include names, addresses, phone numbers, birthdates, social security numbers, tax identification numbers, national insurance numbers and financial account numbers.

3. Scope

The Policy applies to all employees, contractors, consultants and vendors who access, use or control company resources.

4. Policy

4.1 Objectives

- The Company adheres to legal, regulatory and customer privacy requirements.
- The Company collects personally identifiable information when voluntarily submitted by our online and onsite visitors. The information provided is used to fulfil specific requests unless given permission to use it in another manner.
- In connection with the services we provide, the Company may collect the following types of information:
 - Personally Identifiable Information: Names, addresses, email addresses, phone numbers, birthdates, Aadhaar, tax identification, financial account, national insurance numbers, and company information.
 - Cookies: When a visitor views Company websites, a cookie is sent out to the viewer's computer that will identify the visitor's browser. These cookies enable the website to recognize the visitor's computer the next time the visitor views the Company website. These cookies will be used exclusively to collect information concerning the use of the website. Cookies contain no personally identifiable data, so the visitor's personally identifiable information is not collected or retained.
 - User Communications: When a visitor sends an email or other communication to the Company, these communications may be retained in order to process inquiries, respond to requests, and improve overall services.
 - Affiliated Websites: Personal information that a visitor may provide to websites affiliated with the Company may be sent to the Company in order to deliver services to the

Company or other entities affiliated with the Company. The Company processes such information in accordance with the Policy.

- The Company reserves the right to collect and process personal information in the course of providing services to our clients without the knowledge of individuals involved. Where the Company collects personal information from individuals within the Indian region, upon request, the Company will inform them about the types of person information collected from them, the purposes for which it was collected, and uses of the information, and the types of non-agent third parties to which the Company discloses that information.
- As a general rule, the Company will not disclose personally identifiable information except when the Company is required or permitted per customer agreement, law (including pursuant to national security of law enforcement requirements) or otherwise, such as when the Company believes in good faith that the law requires disclosure or other circumstances outlined in this Privacy Policy require or permit disclosure.

- The Company may share information with governmental agencies or other companies assisting in fraud prevention or investigation. The Company may do so when:

Permitted or required by law

- Trying to protect against or prevent actual or potential fraud or unauthorized transactions
- Investigating fraud which has already taken place

This information, however, is not provided to these companies for marketing purposes.

- Permitted transfers of information, either to third parties or within the Company, include the transfer of information within the India region and shall not be moved out of one jurisdiction to another.
- The Company takes reasonable steps to protect personally identifiable information. To prevent unauthorized access or disclosure of personally identifiable information, maintain data accuracy, and support the appropriate use and confidentiality of personally identifiable information, either for its own purposes or on behalf of our clients, the Company has put in place appropriate physical, technical, and managerial procedures to safeguard and secure the personally identifiable information and data the Company possesses.
- The Company collects and maintains personally identifiable information in a manner that is compatible with the purpose for which it was collected and maintained, or as subsequently authorized by an individual or client. To the extent necessary for such purposes, the Company takes reasonable steps to confirm that personal information is accurate and complete with regard to its intended use.
- Whenever the Company is processing personal data, it will take reasonable steps to keep personal data accurate and up-to-date for the purposes for which they were collected. It will provide data subjects with the ability to exercise the following rights under the conditions and within the limits set forth in the law. If you wish to contact us regarding the use of your personal data or want to object in whole or in part to the processing of your personal data, please contact us. If you have provided consent, you may withdraw consent. You may also request, subject to confidentiality obligations, to:

- Access your personal data as processed by the Company.
- Ask for correction or erasure of your personal data.
- Request portability, where applicable, of your personal data, i.e., that the personal data you have provided to the Company, are returned to you or transferred to the person of your choice, in a structured, commonly used and machine-readable format.
- The Company complies with the Privacy regulations set forth by India's IT ACT 2000 regarding the collection, use, and retention of personal information. The Company has certified to the regulators that it adheres to the statutory requirements. If there is any conflict between the terms in this Privacy Policy and the Privacy Principles, the Privacy Principles shall govern.
- The Company utilizes a self-assessment approach to support compliance with this Privacy Policy.
 - The Company periodically verifies that related policies are accurate, comprehensive for the information intended to be covered, prominently displayed, implemented, and are in conformity with the principles of this Privacy Policy.
 - The Company encourages interested persons to raise any concerns with the Company. The Company will investigate and attempt to resolve complaints and disputes regarding use and disclosure of personal information in accordance with the principles contained in this Privacy Policy.
 - If the Company, the Data Protection Authorities, or other qualified government agencies determine that the Company has not complied with this Privacy Policy, the Company shall take appropriate steps to address any adverse effects related to non-compliance and to promote future compliance.
 - If the Company determines an employee is in violation of this Privacy Policy, that employee will be subject to the Company's disciplinary process.
- In the event that the Company merges, is acquired by or sells its assets to a third-party, the Company may disclose personally identifiable information as is reasonably necessary in connection with any such merger, acquisition or sale. Any such party with whom the Company merges or who acquires some of all of the assets of the Company may not have the same or similar privacy guidelines as set forth in this Privacy Policy and may use personally identifiable information in a manner other than as set forth herein.
- This Privacy Policy shall be reviewed annually and updated as necessary to comply with applicable regulations.
- The Company will post any revised Privacy Policy on its website, or a similar website that replaces that website.
- Information obtained from or relating to clients or former clients is further subject to the terms of any privacy notice provided to the client, any contract or other agreement with the client, and application enforcement laws.

- The Company will cooperate with the appropriate regulatory authorities, including local data protection regulatory authorities, to resolve any complaints regarding the transfer of personal data that cannot be resolved between the Company and an individual.

5. Policy Compliance

5.1 Responsibilities

- The CISO is the approval authority for the Privacy Policy.
- The Information Security team is responsible for the development, implementation, and maintenance of the Privacy Policy.
- Company management is accountable for ensuring that the Privacy Policy and associated standards and guidelines are properly communicated and understood within their respective organizational units. Company management is also responsible for defining, approving, and implementing procedures in its organizational units and ensuring their consistency with the Privacy Policy and associated standards and guidelines.
- All individuals, groups, or organizations identified in the scope of the policy are responsible for familiarizing themselves with the Privacy Policy and complying with its associated policies.

6. Policy Enforcement and Compliance

Compliance with the policy is mandatory and CredAvenue Private Limited ('Yubi') department managers shall ensure continuous compliance monitoring within their department. Compliance with the statements of the policy is a matter of periodic review.


Any breach of the policy may constitute a security violation and gives Yubi the right to conduct disciplinary and / or legal action, up to and including termination of employment or business relationship.

7. Document Management

Technological advances and changes in the business requirements will necessitate periodic revisions to documents. Therefore, this document may be updated to reflect changes or define new or improved requirements as and when required and in compliance with the Information Security Program Charter.

I hereby agree and accept the policy.

Employee Name : Harish B

Signature : 

Harish Boskaran (February 27, 2023, 9:27 GMT)

Date : 27-Feb-2023

ISMS Document

Cyber Security Policy

Document Control ID: Yubi-ISP-11

Issued Date: 19-10-22

Published Date: 19-10-22

Confidential and Proprietary Information of CredAvenue Private Limited ('Yubi'). Only expressly authorized for individuals under obligations of confidentiality with Yubi are permitted to review materials in this document. By reviewing these materials, you agree to not disclose these materials to any third party unless expressly authorized by CredAvenue Private Limited and to protect the materials as confidential and trade secret information. Any unauthorized review, retransmission, dissemination, or other use of these materials is strictly prohibited. If you are not authorized to review these materials, please return these materials (and any copies) from where they were obtained. All materials found herein are provided "AS IS" and without warranty of any kind.

DOCUMENT AND RECORD CONTROL

Revision Table

| Date | Version | Brief Description | Author |
|-----------------|---------|------------------------------|--------------------|
| 19-September-21 | 0.1 | Cybersecurity Policy – Draft | Abinesh Athilingam |
| 29-September-21 | 1.0 | Cybersecurity Policy | Abinesh Athilingam |
| 26-September-22 | 1.1 | Formatting changes | Devika Subbaiah |

Approval History

| Date | Version | Approval | Title |
|-----------------|---------|----------|-------------------------|
| 29-September-21 | 1.0 | Approved | Chief Executive Officer |
| 19-October-22 | 1.1 | Approved | CISO |

Important Note: This document is intended solely for the use of the individual or entity to whom it is transmitted to, and others authorized to receive it. It may contain confidential or legally privileged information. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this document is strictly prohibited and may be unlawful. If you have received this document in error, please notify us immediately.

TABLE OF CONTENTS

| | |
|---|----|
| Office of Responsibility | 4 |
| Purpose | 4 |
| Scope | 4 |
| Cyber Security Policy Statement | 4 |
| Email Usage | 5 |
| Protection | 5 |
| Monitoring | 6 |
| Email Signature | 6 |
| Internet Usage Policy | 6 |
| Portable Media | 7 |
| Confidentiality | 7 |
| Human Resources | 8 |
| Access Control | 8 |
| Password | 8 |
| Remote Access | 8 |
| Operations Security | 9 |
| Network Security | 9 |
| Wireless Security | 10 |
| Logging and Monitoring Events | 10 |
| Event Logging and Monitoring | 10 |
| User Monitoring | 10 |
| Workstation Security | 11 |
| Secure Software Development | 11 |
| Patch/Vulnerability & Change Management | 11 |
| Authentication Framework for Customers | 12 |
| Vendor Risk Management | 12 |

| | |
|---|-----------|
| Advanced Threat Protection (Real-Time) | 13 |
| Anti-Phishing | 13 |
| Data Leak Prevention Strategy | 13 |
| Metrics | 13 |
| Roles and Responsibilities | 13 |
| Policy Enforcement and Compliance | 15 |
| Waiver Criteria | 15 |
| ISO 27001 References | 15 |
| Related Policies | 15 |
| Document Management | 16 |

1. Office of Responsibility

Chief Information Security Officer

2. Purpose

The Policy is aligned to the Information Security Program Charter which adheres to the risk management approach for developing and implementing Information Security Policies, standards, guidelines and procedures. This document is to provide details of Yubi's Cyber Security policy that is applicable at CredAvenue Private Limited ('Yubi'). This document has been prepared as per the guidelines by RBI Master Circular. The Master circular requires NBFCs to put in place the following policies

- IT Governance
- IT Policy
- Information Security
- Cyber Security
- IT Operations
- IS Audit
- Business Continuity Planning
- Disaster Recovery Management
- IT Services Outsourcing

3. Scope

The policy applies to all individuals who access, use or control Yubi owned resources. This includes but is not limited to Yubi's employees, third parties (contractors, consultants and other workers including all personnel affiliated to external organizations), investors, customers, other internal and external stakeholders with access to the Yubi's resources, network.

This Policy does not cover issues related to general physical and building security. It covers, however, physical security aspects of buildings or parts of buildings that directly affect the security of information owned by Yubi.

4. Cyber Security Policy Statement

The cyber security policy is an indicative document which serves several purposes including the descriptions for acceptable use of resources. This policy also describes user privilege and responsibilities.

4.1 Email Usage

E-mail is a business communication tool which all employees are requested to use in a responsible, effective and lawful manner. You can find the detailed email usage requirements in the dedicated policy named Email Procedure and Acceptable Use Policy.

Employees should use their company email primarily for work-related purposes.

Employees can use their email to:

- Communicate with current or prospective customers and partners.
- Log in to purchased software they have legitimate access to.
- Give their email address to people they meet at conferences, career fairs or other corporate events for business purposes.
- Sign up for newsletters, platforms and other online services that will help them with their jobs or professional growth.

Inappropriate Usage: Official email should not be used to

- Sign up for illegal, unreliable, disreputable, or suspect websites and services.
- Send unauthorized marketing content or solicitation emails.
- Register for a competitor's services unless authorized.
- Send insulting or discriminatory messages and content.
- Intentionally spam other people's emails, including their co-workers.
- Our company has the right to monitor and archive corporate emails.
- Create or distribute any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.

4.1.1 Protection

- Employees should always be vigilant to catch emails that carry malware or phishing attempts.
- Avoid opening attachments and clicking on links when content is not adequately explained (e.g., "Watch this video, it's amazing.").
- Be suspicious of clickbait titles.
- Check email and names of unknown senders to ensure they are legitimate.
- Look for inconsistencies or style red flags (e.g., grammar mistakes, capital letters, excessive number of exclamation marks.).
- If an employee isn't sure that an email they received is safe, please check with the Infosec team at Infosec@go-yubi.com before proceeding further.

4.1.2 Monitoring

Yubi will monitor all email communication and employees should not expect any privacy whatsoever when using the email system.

4.1.3 Email Signature

Employees must use only Yubi approved signatures as their official emails.

4.1.4 **Internet Usage Policy**

Yubi provides Internet access to all staff to assist them in carrying out their duties such as looking up details about suppliers, products, accessing governmental information and other work-related information.

- Occasional and limited personal use of the Internet is permitted if such use does not:
 - Interfere with work performance & productivity.
 - Include downloading or distribution of large files.
 - Have a negative impact on the performance of IT systems.
- When using Internet access facilities, you should comply with the following guidelines:
 - Keep your personal use of the Internet to a minimum.
 - Check that any information you use from the Internet is accurate, complete and current.
 - Respect the legal protections of data, software, copyright and licenses.
 - Immediately inform the Information Security team of any unusual occurrence.
 - Do not download or transmit text or images which contain any software, material of obscene, threatening, racist or extreme political nature, or which incites violence, hatred or any illegal activity.
 - Do not use the company's equipment to make unauthorized access to any other computer or network.
 - Do not represent yourself as another person.
- It is **STRICTLY FORBIDDEN** to upload Company non-public Information such as any of the following to external file transfer or storage sites, like Box, Dropbox or personal Google Drive:
 - Source Code, object code, user documentation and all other software development details.
 - Project related information.
 - Personally Identifiable Information.
 - Company strategy and business plans.
 - Corporate IT infrastructure arrangements including any log files.
 - Intellectual Property, such as: Copyrights, Patents and Trade Secrets.
 - Employee personal information such as salaries, appraisals, medical records or health care details.

- Any information concerning our clients and prospects including details of our client projects, client proposals, contracts, fees or strategic plans.
- Information related to our clients' customers, including any details stored within Yubi's software products, such as transaction or bank account details.
- Any other company's non-public information.

Internet usage requirements are described in detail in the dedicated policy named Internet Usage Procedure. Users must read this and comply with it.

4.1.5 Portable Media

The use of portable media is only permitted in exceptional circumstances. When portable media is used it should be afforded a level of protection commensurate with the level of risk, up to and including blocking of all read/write operations for the highest of risk environments. The intended purpose is to protect customer and company information from being transferred via unauthorized means.

Yubi reserves the right to inspect and erase portable media that is used on our network.

4.1.6 Confidentiality

- Yubi users must take precautions to protect company information and make all possible efforts to maintain the confidentiality of personal information, business information and other proprietary informational resources.
- Personally Identifiable Information (PII) shall be classified as confidential, as shall any other information flagged as such. Users must not transfer or store confidential information in any location not previously approved and secured by the infrastructure security team.
- Company information must not be stored on the local hard drive of any workstation, but stored only on provided, network-based locations.
- Information Security staff must provide access to information using the principle of least privilege and shall provide access to informational resources on a need-to-know basis.

4.2 Human Resources

- Information security must be covered in the Human Resources (HR) Security Procedure. The HR policies should ensure, as a minimum, that security is adequately covered in job descriptions; those personnel are adequately screened, trained and that confidentiality agreements are signed by all new employees and contractors.
- A training plan and training material must be in place to ensure that the right level of Security Awareness is created and maintained within the organization.
- Software developers and all other relevant personnel involved in the development of software for Yubi are required to undertake secure development training on a periodic basis.
- Upon termination of employment, including the completion of any contract position, the Infrastructure team is responsible for disabling all of the departing employee's user accounts and privileges.

4.3 Access Control

4.3.1 Password

- Users must be forced to change their passwords during the first log on, and at 60-day intervals.
- Passwords shall not be displayed or transmitted in clear text and shall be suitably protected via approved cryptographic solutions. Passwords shall be stored in an encrypted format. A history of passwords shall be maintained to prevent the reuse of passwords. A maximum of six successive login failures shall result in account lockout until an administrator unlocks it. Default accounts shall be disabled and/or default passwords associated with such accounts shall be changed.

4.3.2 Remote Access

- Users may be required to access the Yubi's Information systems from outside the office, for example employees working from home, travelling consultants and/or employees working in Sales / Business Solutions.
- For remote access to the Corporate IT Infrastructure resources only the officially supported and approved facilities by the internal IT department are to be used. The associated security policies must be applied. Online Communication from within Yubi's offices to an external party may only use Yubi's approved communication channels. Personal internet connections or connectivity devices (e.g., using personal data modems and Mobile Hotspot connections, remote access connections, personal VPNs etc.) are strictly prohibited.

The detailed Electronic Communication Requirements are described in the dedicated policy named Communications Security Policy.

4.4 Operations Security

- Yubi's network environment must be segmented to protect and isolate confidential resources. An annual penetration testing to be conducted to stay in compliance with data security standards.
- All changes must be conducted in a controlled and approved way to ordinance with the Operations Security Policy.
- System changes or re-configurations of standard IT components are not allowed. Only additions and/or changes of software components can be made by users on workstations based on customer project requirements. The following system changes are strictly prohibited unless special authorization of the Corporate or local IT Manager has been granted: Installation of:
 - Unauthorized connectivity devices (e.g., data modems)
 - Any component suitable to gain unauthorized access to restricted areas
 - Merging of two networks by physically integrating them on a network node
 - Disabling virus protection

- Any other non-standard software or hardware component

4.5 Network Security

- A secure and trusted network is essential as well as critical to the security of our business.
- External facing networks should be firewalled to an appropriate level.
- Physical and logical network changes should only be made by approved users.
- Networks should be segregated on a regional and/ or business line basis.
- Appropriate controls should be in place at network interfaces.
- WAN services should only be acquired through approved vendors.
- Network event logging and monitoring should be implemented.
- Third-party users shall not connect their computing devices to the wired or wireless network of Yubi, unless authorized.
- Company computers and networks may be connected to third-party computers or networks only with explicit approval after determination that the combined systems will be in compliance with Yubi's security requirements.

4.6 Wireless Security

- Only approved wireless access points should be used.
- Wireless networks should always be encrypted.

4.7 Logging and Monitoring Events

4.7.1 Event Logging and Monitoring

Adequate monitoring controls to detect attacks and unauthorized access to its information processing systems must be implemented. The level of monitoring required shall be determined by risk assessment and any relevant or applicable legal requirements shall be identified to ensure that the monitoring activities comply with the requirements. Monitoring may consist of activities such as the review of:

- Automated intrusion detection system logs
- Firewall logs
- User account logs
- Network scanning logs
- Application logs
- Help desk tickets

- Vulnerability Scanning
- Other log and error files

Any security issues discovered will be reported to the IT Security Department for investigation.

4.7.2 User Monitoring

In order to maintain the security of the Yubi's IT systems (including to prevent cybersecurity threats) and to protect the assets and data, Yubi's IT Security team monitors many aspects of user behaviour including but not limited to:

- Monitoring Internet access usage.
- Reviewing material downloaded or uploaded via the Internet.
- Reviewing emails sent or received by users, provided that there is a well-founded suspicion about a breach of provisions of this Policy or of applicable laws, or if there is a legal or regulatory requirement in this respect.
- Reviewing installed software on user's computers.
- Logins to and use of Company's network as well as use of PCs.

Any monitoring done by Yubi will be in accordance with applicable law.

4.8 Workstation Security

- All workstations (Laptops) must have all Yubi approved security tools pre-installed and fully encrypted.
- Administrator access on the workstation must be controlled with least privilege principles.
- Only install software from trusted sources.
- Do not allow unauthorized users to access your workstation.
- Apply software and virus updates as needed using automated workstation software.
- Take appropriate steps to maintain the physical security of your workstation.

4.9 Secure Software Development

Application Security checkpoints are to be implemented across all stages of software development. It shall include source code audits professionally by having assurance from application providers/OEMs that the application is free from embedded malicious / fraudulent code.

Secure coding guidelines are developed and adhered. Besides business functionalities, security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, session management, security event tracking and exception handling are clearly specified at the initial and ongoing stages of system development/acquisition/implementation.

Proper segregation (logical) shall be available between all stages of software development like development, staging and production.

Software/Application development approach shall be based on threat modelling, incorporate secure coding principles and security testing based on global standards and secures rollout. Like OWASP Top 10, SANS 25 and CIS 20 controls are to be tested.

Containerized application environments shall be prepared and implemented for exclusive business use that is encrypted and separated from other smart phone data/applications; measures to initiate a remote wipe on the containerized app, rendering the data unreadable, in case of requirement may also be considered.

4.10 Patch/Vulnerability & Change Management

Yubi shall follow a documented risk-based strategy for inventorying IT components that need to be patched, identification of patches and applying patches so as to minimize the number of vulnerable systems and the time window of vulnerability/exposure.

Appropriate systems and processes are in place to identify, track, manage and monitor the status of patches to operating system and application software running at end-user devices directly connected to the internet and in respect of Server operating Systems / Databases / Applications / Middleware, etc.

Changes to business applications, supporting technology, service components and facilities are managed using robust configuration management processes, configuration baseline that ensures integrity of any changes thereto.

Periodically conduct VA/PT of internet facing web/mobile applications, servers & network components throughout their lifecycle (pre-implementation, post implementation, after changes etc.).

Periodically conduct Application security testing of web/mobile applications throughout their lifecycle (pre-implementation, post implementation, after changes) in an environment closely resembling or replica of production environment.

As a threat mitigation strategy, identify the root cause of the incident and apply necessary patches to plug the vulnerabilities.

Periodically evaluate the access device configurations and patch levels to ensure that all access points, nodes between (i) different VLANs (ii) LAN/WAN interfaces (iii) Yubi's network to external network and interconnections with partner, vendor and service provider networks are securely configured.

4.11 Authentication Framework for Customers

Implement authentication mechanisms to provide positive identity verification to customers. Customer identity information should be kept secure. Yubi will be the identity provider for identification and authentication of customers for access to partner systems using secure authentication technologies.

4.12 Vendor Risk Management

Yubi shall be accountable for ensuring appropriate management and assurance on security risks in outsourced and partner arrangements. Yubi carefully evaluates the need for outsourcing critical processes like facility management services, desktop management, UPS management etc. And selection of vendor/partner based on comprehensive risk assessment done by the IT team.

Established appropriate framework, policies and procedures supported by baseline system security configuration standards to evaluate, assess, approve, review, control and monitor the risks and materiality of all its vendor/outsourcing activities are in place.

Reserve Bank of India shall have access to all information resources (online/in person) that are consumed by us, to be made accessible to RBI officials by the Yubi when sought, though the infrastructure/enabling resources may not physically be located in the premises.

Further, Yubi adheres to the relevant legal and regulatory requirements relating to geographical location of infrastructure and movement of data out of borders. Background checks, non-disclosure and security policy compliance agreements are mandated for all third-party service providers.

4.13 Advanced Threat Protection (Real-Time)

A robust perimeter defence shall be in place to protect against the installation, spread, and execution of malicious code at multiple points in the enterprise.

Yubi shall have Anti-malware, Antivirus protection including behavioral detection systems for all categories of devices – (Endpoints such as PCs/laptops/ mobile devices etc.), servers (operating systems, databases, applications, etc.), Web/Internet gateways, email-gateways, Wireless networks, SMS servers etc. Including tools and processes for centralized management and monitoring.

4.14 Anti-Phishing

Yubi shall subscribe at firewall level for Anti-phishing/anti-rouge app services from external service providers for identifying and taking down phishing websites/rouge applications.

4.15 Data Leak Prevention Strategy

Yubi shall have a comprehensive data loss/leakage prevention strategy at firewall level to safeguard sensitive (including confidential) business and customer data/information.

This includes protecting data processed in end point devices, data in transmission, as well as data stored in servers and other digital stores, whether online or offline.

4.16 Metrics

Yubi shall develop a comprehensive set of metrics that provide for prospective and retrospective measures, like key performance indicators and key risk indicators. Few illustrative metrics included coverage of anti-malware software and their updating percentage, patch latency, extent of user awareness training, vulnerability related metrics, etc.

5. Roles and Responsibilities

Each role involved in this policy shall have main responsibilities as follows:

Information Security Team

- Managing and implementing this policy and related policies, standards and guidelines.
- Monitoring and responding to potential and/or actual IT security breaches.
- Ensuring that staff are aware of their responsibilities and accountability for information security.

- Act as a consulting contact for all security related issues.
- Act as a central point of contact on Information Security for both staff and external organizations.
- Acts as an approval authority for the Information Security policy and its exceptions.

Chief Information Security Officer

- Review and signoff changes to Information Security policies
- Responsible for information risk within Yubi advising the executive management on the effectiveness of management of security and privacy issues across the organization and advising on compliance with relevant legislation and regulations.
- Responsible for cascading and ensuring the implementation, operation, monitoring, maintenance and improvement of the Information Security Management System.

Managers

- Ensuring that the Information Security policy and associated standards and guidelines are properly communicated and understood within their respective organizational units.
- Defining, approving and implementing procedures in their organizational units and ensuring their consistency with the Information Security Policy and associated standards and guidelines.
- Determining the level of access to be granted to specific individuals.
- Ensuring staff have appropriate training for the systems they use.
- Ensuring staff know how to access advice on information security matters.

All Employees

All individuals, groups, or organizations identified in the scope of this policy are responsible for familiarizing themselves and complying with the Information Security Policy and associated standards and procedures.

All employees are responsible for information security and therefore must understand and comply with this policy and associated guidance. Failure to do so may result in disciplinary action.

In particular, all employees should understand:

- What information they are using, how it should be used, stored and transferred in terms of data security
- What procedures, standards and protocols exist for the sharing of information with other parties
- How to report a suspected breach of information security within the organization
- Their responsibility for raising any information security concerns

All individuals are responsible for adhering to the provisions of this Policy and all related policies, standards, guidelines and procedures and must report every incident of misuse or abuse of which they become aware as described in this policy.

6. Policy Enforcement and Compliance

Yubi recognizes its burden to exercise due care for the safeguarding of data in its custody including, but not limited to, Personally Identifiable Information (PII), Financial information and Yubi Intellectual Property. To this end, and for overall assurance of the confidentiality, integrity, and availability of Yubi information systems, an independent review of compliance with this Policy shall be conducted on a regular basis.

Yubi must adhere to applicable Reserve Bank of India's (RBI) Master directions for Non-Banking Financial Companies and RBI's IT Framework. This is not intended to be an exhaustive list of applicable regulatory requirements with respect to state or local laws that must similarly be complied with.

Further, all employees shall comply with relevant national and local legal, regulatory, and contractual requirements. Any Yubi employee who does not comply with this policy may be subject to disciplinary action, up to and including termination. Access to Yubi information systems and resources is a privilege, not a right, and may be revoked or suspended at any time.

7. Waiver Criteria

The policy is intended to address information security requirements. If needed, waivers shall be formally submitted to the Information Security Management, including justification and benefits attributed to the waiver by the CISO.

The policy waiver shall be granted for a period of four months initially and shall be reassessed thereafter and can be extended up to a period of three consecutive terms. No waiver shall be provided for more than three consecutive terms on any of the policies.

8. ISO 27001 References

- A. 5.1.1 Policies for Information Security
- A. 5.1.2 Review of the Policies for Information Security
- Clause 5.1 Leadership and commitment
- Clause 5.2 Policy

9. Related Policies

- Acceptable Use Policy
- Clear Desk and Clear Screen Policy
- Access Control Policy
- Asset Management Policy
- Legal and Compliance Policy
- Information Security Policy


- Risk Management Policy

10. Document Management

Technological advances and changes in the business requirements will necessitate periodic revisions to documents. Therefore, this document may be updated to reflect changes or define new or improved requirements as and when required and in compliance with the Information Security Program Charter.

I hereby agree and accept the policy.

Employee Name : Harish B

Signature : 

Harish Baskaran (February 27, 2023, 9:27 GMT)

Date : 27-Feb-2023

ISMS Document

Acceptable Use Policy

Document Control ID: Yubi-ISP-04

Issued Date: 19-10-22

Published Date: 19-10-22

Confidential and Proprietary Information of CredAvenue Private Limited ('Yubi'). Only expressly authorized for individuals under obligations of confidentiality with Yubi are permitted to review materials in this document. By reviewing these materials, you agree to not disclose these materials to any third party unless expressly authorized by CredAvenue Private Limited and to protect the materials as confidential and trade secret information. Any unauthorized review, retransmission, dissemination, or other use of these materials is strictly prohibited. If you are not authorized to review these materials, please return these materials (and any copies) from where they were obtained. All materials found herein are provided "AS IS" and without warranty of any kind.

DOCUMENT AND RECORD CONTROL

Revision Table

| Date | Version | Brief Description | Author |
|-----------------|---------|-------------------------------|--------------------|
| 07-September-21 | 0.1 | Acceptable Use Policy – Draft | Abinesh Athilingam |
| 29-September-21 | 1.0 | Acceptable Use Policy | Abinesh Athilingam |
| 26-September-22 | 1.1 | Formatting changes | Devika Subbaiah |

Approval History

| Date | Version | Approval | Title |
|-----------------|---------|----------|-------------------------|
| 29-September-21 | 1.0 | Approved | Chief Executive Officer |
| 19-October- 22 | 1.1 | Approved | CISO |

Important Note: This document is intended solely for the use of the individual or entity to whom it is transmitted to, and others authorized to receive it. It may contain confidential or legally privileged information. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this document is strictly prohibited and may be unlawful. If you have received this document in error, please notify us immediately.

TABLE OF CONTENTS

| | |
|--|----------|
| Office of Responsibility | 3 |
| Purpose | 3 |
| Scope | 3 |
| Policy | 3 |
| Objectives | 3 |
| Confidentiality/Non-Disclosure | 4 |
| Acceptable Use Core Principals | 4 |
| Related Policies | 6 |
| Policy Compliance | 6 |
| Responsibilities | 6 |
| Policy Enforcement and Compliance | 6 |
| Waiver Criteria | 7 |
| Document Management | 7 |

1. Office of Responsibility

Chief Information Security Officer

2. Purpose

As stated in the Company Information Security Program Charter, the Company will follow a risk management approach to developing and implementing Information Security policies, standards, guidelines, and procedures. The Information Security Program is designed to protect information assets by developing Information Security policies to identify, classify, and define the acceptable use of company information assets.

The Acceptable Use Policy defines company objectives for establishing specific standards on appropriate business use of the company's information and telecommunications systems and equipment.

3. Scope

The Policy applies to all employees, contractors, consultants and vendors who access, use or control company resources.

4. Policy

4.1 Objectives

- The Company information systems, telecommunications systems, and equipment; including but not limited to: Internet/Intranet/Extranet-related systems, computer equipment, software, operating systems, storage media, mobile devices, electronic mail, telephone, pager, voice mail, and fax, are provided for official and authorized Company business purposes. Any use of such systems and equipment perceived to be illegal, harassing, offensive, or in violation of other Company policies, standards or guidelines, or any other uses that would reflect adversely on the Company; may be considered a violation of this policy.
- Inappropriate use of these resources may expose the company to risks including virus attacks, compromise of network systems and services, and legal issues.
- Actual or suspected misuse of these systems shall be reported to the appropriate Company management representative in a timely manner.
- The company has defined the thresholds of acceptable use in multiple policy documents. Acceptable usage requirements include but are not limited to:
- Explicit management approval (authorization) to utilize company technology and information as needed to fulfil job functions.
- Required authentication for use of company technology and information.
- Acceptable usage of company technology and information including inappropriate access by non-authorized individuals (e.g., unauthorized colleagues, neighbours, relatives, etc.)
- Acceptable network locations and remote access requirements for company technology and information.
- List of company-approved products, services for usage, and the storage of company data.

- Prohibition of storage of sensitive company or client data on unauthorized media including but not limited to, local hard drives, floppy disk drives, portable hard drives, flash drives, mobile cellular devices, or other external media, etc. without a documented business justification and explicit documented approval from Information Security & Risk.
- Authorization to access or utilize company technology and information must be approved by each employee's manager and documented. If any unauthorized activity is identified by monitoring or other means; this activity shall be brought to the attention of the employee's manager to determine the appropriate disciplinary and/or legal action.
- Where the company collects data, including sensitive personal data, as defined in the Data Protection and Security Policy, it shall do so in accordance with the Data Protection and Security Policy. Such collection may include monitoring and/or recording employees' use of information, telecommunication systems and equipment including the use of the internet, electronic mail, telephone, voicemail, and fax technologies. The Company shall obtain the required consent of employees for data collection and monitoring.

4.2 Confidentiality/Non-Disclosure

- The Company confidentiality and non-disclosure agreements shall be designed to address the requirements needed to protect confidential information using legally enforceable terms. Company confidentiality/non-disclosure agreements are applicable to all personnel, contractors, and vendors/third party service providers and execution is required prior to the initiation of any employee or third-party services. Company confidentiality and on-disclosure agreements shall include a specific set of requirements governing the access and use of company confidential information and client information including but not limited to financial transactional information, and personally identifiable information.
- Requirements for confidentiality and non-disclosure agreements shall be reviewed at least annually and when changes occur that influence these requirements, such as applicable laws and regulations for the jurisdiction to which they apply.
- A list of representatives who are authorized to sign confidentiality and non-disclosure agreements on behalf of the company shall be published, maintained, and updated to reflect personnel changes and departures.

4.3 Acceptable Use Core Principals

- All employees shall complete mandatory security awareness (including privacy), and compliance training within 30 days of hire, and annually thereafter.
- Documented explicit management approvals are required before employees can be granted access to or assigned the use of any Company information system or device.
- All access to or use of Company technology requires authentication. Access to any Company system or network constitutes acknowledgment of and consent to monitoring. The company reserves the right to audit networks and information systems on a periodic basis to ensure compliance with the company policy. All employees shall be assigned a unique account. Employees are prohibited from sharing account usernames or passwords with anyone. All employees are required to use company resources only as authorized and as necessary to fulfill assigned job duties.
- Access to Company technology, along with any information received or processed by Company is restricted to designated Company employees or authorized recipient access only. Exposure to or use by employee relatives, neighbors, or otherwise is explicitly prohibited and is deemed inappropriate. All employees have a responsibility to promptly

report theft, loss, or unauthorized access to company resources immediately upon discovery.

- All employees are required to access Company resources only from approved/authorized network locations. The approval to Telework must be approved by an employee's direct supervisor. Company network resources will only be accessed via the secure options configured by the enterprise network staff.
- Any personal home networks (wired or wireless) utilized during authorized Telework activities must be secured at all times (not open to public) when in use for company business, and anytime company equipment is connected. Employees are required to utilize the secure company configured VPN options to access enterprise network resources during Telework efforts.
- All employees shall adhere to the use of company approved programs and shall not attempt to access or install any programs without prior approval. The installation of company approved programs shall be completed by an approved/authorized system administrator. Employees must adhere to copyright laws including but not limited to laws governing, photographs, music, and the installation of any copyrighted software.
- All mobile devices authorized by the company to conduct company business shall be protected from unauthorized access; these devices shall be configured with active password/passcode and properly safeguarded as defined in the company policies. Company-provided and authorized mobile devices (laptops, cellphones, etc.) shall not be left unattended in public areas such as, but not limited to cars, hotel rooms, conference rooms, and airports.
- Company-provided mobile devices (laptops, cellphones, etc.) are not authorized to access production areas of the network that processes client data.
- All employees shall lock systems or log off when they are away from their work area, or their workstation is left unattended.
- The storage of client information including but not limited to; Credit card information, PII (Personally Identifiable Information) and any other sensitive data on non-production hard drives, laptops, portable media, flash drives, floppy disks, mobile devices, or other unauthorized external media is strictly prohibited.
- Employees shall use extreme caution when opening email attachments or clicking links in messages received from unknown senders, which may introduce malware into the company environment. Employees are prohibited from sending or receiving email content with pornographic, obscene, sexually related, profane or offensive material or language.
- Employees shall refrain from referencing the company or any of its employees, the company's customers, customer information, or security practices on any social media platform.
- Employees are prohibited from making any discriminatory, disparaging, defamatory or harassing comments on any social media platform or otherwise engaging in any conduct prohibited by the Company Code of Conduct policy.

5. Related Policies

- Information Security Program Charter
- Data Protection and Security Policy

6. Policy Compliance

6.1 Responsibilities

- The CISO is the approval authority for the Acceptable Use Policy
- The Information Security team is responsible for the development, implementation, and maintenance of the Acceptable Use Policy.
- Company management is accountable for ensuring that the Acceptable Use Policy and associated standards and guidelines are properly communicated and understood within their respective organizational units. Company management is also responsible for defining, approving, and implementing procedures in its organizational units and ensuring their consistency with the Acceptable Use Policy and associated standards and guidelines.
- All individuals, groups, or organizations identified in the scope of this policy are responsible for familiarizing themselves with the Acceptable Use Policy and complying with its associated policies.

7. Policy Enforcement and Compliance

Compliance with this policy is mandatory and CredAvenue Private Limited ('Yubi') department managers shall ensure continuous compliance monitoring within their department. Compliance with the statements of this policy is a matter of periodic review.

Any breach of this policy may constitute a security violation and gives Yubi the right to conduct disciplinary and / or legal action, up to and including termination of employment or business relationship.

Disciplinary action will be dependent upon the severity of the violation which will be determined by the investigations.

8. Waiver Criteria

The policy is intended to address information security requirements. If needed, waivers shall be formally submitted to the Information Security Management, including justification and benefits attributed to the waiver by the CISO.


The policy waiver shall be granted for a period of four months initially and shall be reassessed thereafter and can be extended up to a period of three consecutive terms. No waiver shall be provided for more than three consecutive terms on any of the policies.

9. Document Management

Technological advances and changes in the business requirements will necessitate periodic revisions to documents. Therefore, this document may be updated to reflect changes or define new or improved requirements as and when required and in compliance with the Information Security Program Charter.

I hereby agree and accept the policy.

Employee Name : Harish B

Signature : 

Harish Baskaran (February 27, 2023, 8:27 GMT)

Date : 27-Feb-2023

ISMS Document

Laptop Security Policy

Document Control ID: Yubi-ISP-25

Issued Date: 19-10-22

Published Date: 19-10-22

Confidential and proprietary information of Credavenue Private Limited ("CAPL" or "Company"). Only expressly authorized individuals under obligations of confidentiality with CAPL are permitted to review materials in this document. By reviewing these materials, you agree to not disclose these materials to any third party unless expressly authorized by CAPL and to protect the materials as confidential and trade secret information. Any unauthorized review, retransmission, dissemination, or other use of these materials is strictly prohibited. If you are not authorized to review these materials, please return these materials (and any copies) from where it was obtained. All materials found herein are provided "AS IS" and without warranty of any kind.

DOCUMENT AND RECORD CONTROL

Revision Table

| Date | Version | Brief Description | Author |
|--------------|---------|---------------------------------|--------------------|
| 16-August-21 | 1.0 | Laptop Security Policy creation | Abinesh Athilingam |

Approval History

| Date | Version | Approval | Title |
|---------------|---------|----------|-------|
| 19-October-22 | 1.0 | Approved | CISO |

TABLE OF CONTENTS

| | |
|--|-----------|
| Office of Responsibility | 5 |
| Purpose | 5 |
| Scope | 5 |
| Policy | 5 |
| Related Policies | 9 |
| Policy Compliance | 9 |
| Responsibilities | 9 |
| Policy Enforcement and Compliance | 10 |
| Waiver Criteria | 10 |
| Document Management | 10 |

1. Office of Responsibility:

Chief Information Security Officer

2. Purpose:

The Laptop(s) allows the authorized employees and other users of the CAPL and its subsidiaries to have their computing resource at hand in meetings/workplace or even at home in certain time pressing situations so as to enable employees to be maximally functional and productive while away from office.

This Laptop policy ("Policy") describes the necessary controls to minimize information security risks and physical damages to an issued Laptop. Laptop devices make itself vulnerable to physical damages and theft as its highly portable. The impact of such damage not only includes just the replacement value of the hardware and software but also the value of the organizational data stored in such Laptop, or accessible through such Laptop.

3. Scope:

This Policy applies to all employees, contractors, consultants, interns and vendors (collectively herein referred to as "Users") who access or use official Laptop as may be issued by CAPL. In addition to this Policy, employees are also required to adhere to the Acceptable Use Policy and any terms and conditions as mentioned in their respective employment agreement.

Any User using Laptop issued by CAPL is responsible for the security of such Laptop, regardless of the fact whether such Laptop is used in the office, at one's place of residence, or in any other location such as a hotel, conference room or while traveling. This Policy contains certain guidelines and restrictions on the usage of the Laptop that are required to be strictly adhered to by all the Users while using these Laptops.

4. Policy:

Intended Use of Laptops

Laptop shall always be the property of the Company and the Users shall not have any right or interest in the said asset except using such asset during the course of employment or for such duration as may be decided by the Company. Users must ensure that the Laptop is being used only for official purposes and during the rightful discharge of their duties and not for generating, transmitting, corresponding any content that is contrary to Company policies as may be issued from time to time and usage for personal activities are limited to a very minimal extent with approvals.

Any violation of the preceding paragraph, may result in User being subject to disciplinary or any other appropriate action as per Company policies as may be issued from time to time.

Laptop Security Controls

All Laptops issued to the Users by the Company shall be the Company's property. Each User issued with a Laptop shall be responsible for the security of that Laptop, regardless of whether such Laptop is used in the office, at the employee's place of residence, or in any other location not limited to a hotel, conference room, car or airport. Users shall ensure security of the Laptop in each of the following domains as per the Company policies as may be issued from time to time. Laptops must compulsorily be protected by a domain username and password. Usage of local users (non-domain) accounts on the Laptop is strictly restricted.

Handling and protecting the Laptops from physical damage & theft

It is mandatory for the Users to always keep the Laptops at safe custody during the possession of the Laptop. All Users are required to undertake the following actions:

1. The physical security of the Laptops is the User's responsibility. Such Users are therefore required to take all reasonable precautions, be sensible and stay alert to the risks.
2. Users should keep the Laptop in their possession and within a close sight whenever possible. Users to be extra careful in public places such as airports, railway stations or restaurants to avoid stealing.
3. Users shall never leave the laptop unattended when using it outside the office premise.
4. Users shall lock the Laptop when not in use, preferably in a strong cupboard, filing cabinet or safe. This applies at home, in the office or in a hotel.
5. Users shall never leave a Laptop unattended in a vehicle. If necessary, keep it in the trunk or glove box but it is generally much safer to carry it, wherever possible.
6. Carry and store the Laptop in a padded laptop bag or strong briefcase to reduce the chance of accidental damage.
7. Users may not take the Laptop for repair to any external agency or vendor at any point of time.
8. In case of any failure, Users are required to report the same to the management.
9. In case of loss of Laptop whether on-premise or off premise of the Company, due to negligence of the User, the Company may recover the cost of such Laptop from such User. It is the Company's discretion to impose further penalties on account of loss of sensitive Company's or its clients information including confidential information stored in such Laptop.
10. If there is a damage on account of the above mentioned point, the User may be liable to pay the damages at cost to the Company and the same may be deducted from their monthly salary.
11. Company maintains the right to conduct inspections of any Laptop without prior notice to its User. The User shall submit the Laptop for random audit by the Company in order to check the physical presence as well as the functional usability of the Laptop.
12. In case of termination or cessation of the employment, the User shall hand over the Laptop to the Company in good condition failing which Company is authorized to charge penalty against the User at its own discretion.
13. If a Laptop is lost or stolen it must be reported to the IT department of the Company immediately. Theft or loss of Laptop outside Company's premises should also be reported at the nearest local police station and First Information Report (FIR) must be lodged at the earliest. The FIR should include the serial number for the lost Laptop, which can be obtained from the IT department of the Company. A copy of the FIR must be submitted to the IT department within 48 hours and User can also seek help from the administration department of the Company.

Protecting the Data in the Laptop:

The Users are expected to ensure the security of the data within their Laptops. In this regard Users are to adhere to the following:

- o Users are personally accountable for all network and systems access under your user ID, so keep passwords absolutely secret. Never share it with anyone, not even members of your family, friends, or IT staff.
- o Laptops are provided for official use to authorized Users. Do not loan Laptop or allow it to be used by others such as family and friends.
- o Avoid leaving the laptop unattended and logged-on. Always shut down, log off or activate a password-protected screensaver before walking away from the Laptop.

Prevent malicious contents:

- o Email attachments are now the bigger security threat as it's used in ransomware attacks. Avoid opening any email attachment unless Users are expecting to receive it from a known/verified source.
- o Always virus-scan any files downloaded to User's Laptop from any source (CD/DVD, USB hard disks and memory sticks, network files, email attachments or files from the internet). Virus scans normally happen automatically in your User's Laptop. If not sure, get that checked with the IT support team.
- o Report any security incidents (such as virus infections) promptly to the IT support team in order to minimize the damage or loss of data.
- o Respond immediately to any virus warning message on the User's Laptop, or if you suspect a virus (e.g. by unusual file activity) by contacting the IT Support team. Do not forward any files or upload data onto the network if the User suspects that the User's Laptop is infected.

Data Backups

User shall be personally responsible for storing their data in Google drive or such drive as may be identified by the Company.

Do note that if the laptop is stolen, lost or damaged, or malfunctioned, it may be impossible to retrieve any of the data from the Laptop. Saving the data in Google drive shall save a lot of effort and extra work of the User.

Use of Unauthorized Software /Content

- o Users are required to ensure that they do not download, install or use unauthorized software programs. Unauthorized software could introduce serious security vulnerabilities into the Company's networks as well as affecting the working of the User's Laptop. Software packages that permit the User's Laptop to be 'remote controlled' (e.g. PCAnywhere) and 'hacking tools' (e.g. network sniffers and password crackers) are explicitly forbidden on User's Laptop unless they have been explicitly pre-authorized by Company management for furtherance of legitimate business purposes of the Company.
- o All software or other programs that are downloaded onto the Company provided Laptop, whether or not they are so downloaded in accordance with the business needs of the Company, or the directions of the Company's management in this regard, shall immediately become the sole and exclusive property of the Company, and henceforth can only be used in accordance with the directions of the Company in this regard. Further, any programs or software that were pre-installed at the time of the possession of the Laptop being handed

over to the Company, cannot be altered or removed, whether permanently or temporarily, in any manner whatsoever save and otherwise than in accordance with the directions of the Company in this regard.

- o The User shall not install any unauthorized accessories/software like messengers, chatting software or any malicious software, which may cause problems to the functioning of the Laptop and strictly adhere to Company's software.
- o If there is damage on account of the above, the User may be liable to pay the damages at cost to the Company/the same will be deducted from their monthly salary.
- o As User might expect, Company will not tolerate inappropriate materials such as pornographic, racist, defamatory or harassing files, pictures, videos or email messages that might cause offence or embarrassment to either the Company, its employees or any third party. No User should ever store, use, copy or circulate such material on the Laptop and should not visit or attempt to visit any dubious websites. The Company's IT team shall routinely monitor the Company network and systems for such materials and track use of the internet by all Users. Such IT team shall report serious/repeated offenders and any illegal materials directly to Information security team and Company's management, and appropriate disciplinary processes shall be initiated against such Users by the management.
- o All Users are advised that any information in digital or electronic form that they come across in the Laptop, whether at the time of receiving such Laptop or at any time thereafter, shall be compulsorily treated by such Users as confidential information ("Confidential Information"). Such Confidential Information can exist in any electronic form, including but not limited to documents, memoranda, spreadsheets, databases, encrypted data, passwords, lists of any nature, source code, object code, algorithms, software programs, emails and other communications, designs, blueprints, business projections and plans, financial data, customer and client names and contacts, supplier names and contacts, price lists and quotations, contractual documents, term sheets and executed agreements with vendors/suppliers and customers, and so on. Users cannot use such Confidential Information in any manner whatsoever save and otherwise than in strict accordance with the directions of the Company on this behalf. Any unauthorized usage by the User of such Confidential Information, or any act of omission or commission of the User which results in such unauthorized usage of Confidential Information by any third party, shall expose the User concerned to liability and consequent action by the Company and/or its management.
- o Further, in the event any User is unsure of the status of any digital/electronic information that he or she may discover on the Laptop, the User must forthwith and without any further delay communicate the existence of such information to the Company's IT team on the assumption that all such information is potentially Confidential Information, and thereafter follow the instructions of the IT team in this regard. Under no circumstances shall the User attempt to process such Confidential Information in any manner whatsoever for his or her own personal usage, and any delay in contacting the IT team in this regard shall be regarded as dereliction of duty by the employee.

Replacement of Laptop/Accessories

1. Existing Laptops or its accessories can be replaced by newer ones in the following cases:
 - a. The Laptops are more than four years old and out of the guarantee/ warranty period;
 - b. In an unlikely event of the Laptop becoming unusable (This needs to be confirmed by the IT helpdesk).

- c. In case the current Laptop does not meet the business requirements (This needs to be confirmed by the IT helpdesk)
 - d. If the Laptop and its accessories are damaged beyond repair due to any accident or any other unforeseen circumstances.
2. If the Laptop and/or its accessories are lost due to theft, burglary, any other unforeseen circumstances, the Company shall provide the concerned User with a replacement.

However, the procedure as specified under “**Handling and protecting the Laptops from physical damage & theft**” shall be applicable

3. In case the Laptop is replaced because of reason, the Laptop may be issued to another User. An existing (not necessarily new) Laptop that meets business requirements may be provided to the said User. If the Laptop and/or accessories are replaced because of reason 1 (d), IT helpdesk will evaluate the condition and certify the necessity for replacement. If the damage is due to gross negligence or carelessness, the Company reserves the right to recover the amount incurred for such replacement. If the replacement is as per the provisions of point 2 above, then the Company shall replace at its cost and shall recover a minimum amount as prescribed by the insurance provider beyond its coverage terms.
 4. Any accessory such as power cord, battery and any other parts in the Laptop including display screens may be replaced by IT as needed in consideration with the health and safety aspects. In case if a replacement is not under warranty, then the User shall bear the costs of such replacement.

Breach of compliance to this Policy

Any action of the User that are inconsistent with this Policy shall be treated as serious professional misconduct on the part of the User, and the User concerned shall be subject to any disciplinary proceeding, or action, by the Company, which the management of the Company may deem appropriate under the existing circumstances. Such action may also include any rights of termination or any other rights that the Company may have under the terms of the employment agreement or engagement agreement (as may be applicable) entered into by the Company with the concerned User.

Users are further advised that in the event any such User fails to adhere to the requirements of Laptop usage and restrictions on usage of Confidential Information, he or she shall be subject to any penal action under the relevant provisions of the Information Technology Act, 2000 (the “Act”).

The Company shall bear expenses for Laptop maintenance and repairs arising out of the normal wear and tear. However, in the event of any damage to the Laptop arising out of the negligence, misuse or abuse of the Laptop by the User, the User shall be solely liable to make the payment for all the expenses arising therefrom. The Company shall have the right to reclaim such expenses and deduct the same from your monthly salary.

5. Related Policies:

- Information Security Policy
- Cyber Security Policy
- Asset Management Policy
- Asset Protection Policy

- Asset Identification and Classification Policy
- Acceptable Use Policy

6. Policy Compliance:

6.1 Responsibilities

- The CISO is the approval authority for the Laptop Security Policy.
- The Information Security team is responsible for the development, implementation, and maintenance of the Laptop Security Policy.
- The Company management is accountable for ensuring that the Laptop Security Policy and associated standards and guidelines are properly communicated and understood within their respective organizational units. Company management is also responsible for defining, approving, and implementing procedures in its organizational units and ensuring their consistency with the Laptop Security Policy and associated standards and guidelines.
- All individuals, groups, or organizations identified in the scope of this policy are responsible for familiarizing themselves with the Laptop Security Policy and complying with its associated policies

7. Policy Enforcement and Compliance

Compliance with this policy is mandatory and CredAvenue Private Limited ('Yubi') department managers shall ensure continuous compliance monitoring within their department. Compliance with the statements of this policy is a matter of periodic review.

Any breach of this policy may constitute a security violation and gives Yubi the right to conduct disciplinary and / or legal action, up to and including termination of employment or business relationship.

Disciplinary action will be dependent upon the severity of the violation which will be determined by the investigations.

8. Waiver Criteria

The policy is intended to address information security requirements. If needed, waivers shall be formally submitted to the Information Security team, including justification and benefits attributed to the waiver by the CISO.


The policy waiver shall be granted for a period of four months initially and shall be reassessed thereafter and can be extended up to a period of three consecutive terms. No waiver shall be provided for more than three consecutive terms on any of the policies.

9. Document Management

Technological advances and changes in the business requirements will necessitate periodic revisions to documents. Therefore, this document may be updated to reflect changes or define new or improved requirements as and when required and in compliance with the Information Security Program Charter.

I hereby agree and accept the policy.

Employee Name : Harish B

Signature : 

Harish Baskaran (February 27, 2023, 8:27 GMT)

Date : 27-Feb-2023

ISMS Document

Clean Desk & Clean Screen Procedure

Document Control ID: Yubi-ISPR-01.02

Issued Date: 19-10-22

Published Date: 19-10-22

Confidential and Proprietary Information of CredAvenue Private Limited ('Yubi'). Only expressly authorized for individuals under obligations of confidentiality with Yubi are permitted to review materials in this document. By reviewing these materials, you agree to not disclose these materials to any third party unless expressly authorized by CredAvenue Private Limited and to protect the materials as confidential and trade secret information. Any unauthorized review, retransmission, dissemination, or other use of these materials is strictly prohibited. If you are not authorized to review these materials, please return these materials (and any copies) from where they were obtained. All materials found herein are provided "AS IS" and without warranty of any kind.

DOCUMENT AND RECORD CONTROL

Revision Table

| Date | Version | Brief Description | Author |
|-----------------|---------|---|--------------------|
| 30-September-21 | 0.1 | Clean Desk & Clear Screen Procedure – Draft | Abinesh Athilingam |
| 04-October-21 | 1.0 | Clean Desk & Clear Screen Procedure | Abinesh Athilingam |
| 26-September-22 | 1.1 | Formatting changes | Devika Subbaiah |

Approval History

| Date | Version | Approval | Title |
|---------------|---------|----------|-------------------------|
| 04-October-21 | 1.0 | Approved | Chief Executive Officer |
| 19-October-22 | 1.1 | Approved | CISO |

Important Note: This document is intended solely for the use of the individual or entity to whom it is transmitted to, and others authorized to receive it. It may contain confidential or legally privileged information. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this document is strictly prohibited and may be unlawful. If you have received this document in error, please notify us immediately.

TABLE OF CONTENTS

| | |
|--|----------|
| Office of Responsibility | 3 |
| Purpose | 3 |
| Scope | 3 |
| Clear Desk Procedures | 3 |
| Clear Screen Procedures | 4 |
| Risk Management | 5 |
| Compliance | 5 |
| Responsibilities | 5 |
| Policy Enforcement and Compliance | 5 |
| Waiver Criteria | 6 |
| Document Management | 6 |

1. Office of Responsibility

Chief Information Security Officer

2. Purpose

To improve the confidentiality and security of information, the Clear Desk and Clear Screen Procedure ensures that all sensitive and confidential information, be it on paper, white board, computer storage or hardware device, in trash bin, is securely locked away and/ or disposed of in appropriate manner when not in use.

The Clear Desk and Clear Screen Procedure inform employees, contractors, consultants, vendors, third party employees of their responsibilities and to provide guidance on managing their working environment, workstations, and desks in an appropriate way to:

- Reduce risk of security breach, fraud, and information theft.
- Ensure CredAvenue Private Limited ('Yubi') is compliant with the Data Protection Act, which requires that Yubi's confidential information be kept safe and secure.
- Ensure that all forms of information used in or around a work area is protected from unauthorized viewing or altering while that area is unattended.
- To prevent unauthorized access to systems, data, facilities, and networks.
- To prevent any misuse of or damage to documents and data.
- To mitigate loss or destruction of information in case of a disaster such as fire.

3. Scope

The Clean desk and Clear Screen Procedure apply to all employees, contractors, consultants and vendors who access, use or control company resources.

4. Clear Desk Procedures

In any circumstance when an employee has to leave any data unattended, they must assess the likely risk to the data by others and must act to reduce the risk when leaving their desk. Always consider whether it will be possible for documents on it to be seen or data accessed by those not authorized to do. Whenever possible, employees should clear away and secure any information including, but not limited to, work papers and removable media before leaving their desks.

In particular, the following categories of information must never be left accessible on an unattended desk or workstation and particular care must be taken when printing such material, to ensure that it is promptly removed. It is the policy that all employees should manage their desks in such a way that the following types of information are properly protected:

- Any sensitive, confidential, or restricted information must be removed from the desk and locked in a drawer or in a filing cabinet when the desk is unoccupied and at the end of the workday.
- Even while the employee is at the workstation, paper documents containing sensitive information must be shielded from the view of passers-by or office visitors.

- Filing cabinets containing classified information must be locked when not in use or when not attended.
- Passwords must not be written down and stored near a computer or in any other accessible location (e.g., Notepad, Sticky notes (both paper and app based)).
- Copies of documents containing confidential information must be immediately removed from printers/fax machines. When receiving sensitive facsimile messages users must be physically present to receive the same. Photocopier's fax and telex machines will be locked or protected from unauthorized use outside normal working hours.
- Documents or magnetic media, or other removable media such as CDs, DVDs etc. should be safely stored and kept away from easy access.
- Restricted or confidential information must not be put up on pin up boards or on notice boards and must be locked securely in desks, filing cabinets or rooms at all times, unless they are currently in use.
- Any information written on white boards must be cleared immediately after the meeting is over.
- Restricted information printed on paper, shall be shredded when not in use.

5. Clear Screen Procedures

When leaving the desk and /or workstation unattended, or in any circumstances when a desk or workstation is left vacant in such a way that information left on it could be seen by others, all employees, third parties and vendors should ensure that their computer screen is locked so that information contained in the computer cannot be accessed by anyone else.

- Users are instructed to shut down their computers at the end of the working day.
- Locking the screen not only prevents someone else from using the computer, which is logged on in the user's name, but it also prevents someone from reading classified information left open on the screen, so all users are instructed to lock the computer screen when not attended.
- Lock workstations (computers, laptops, and windows terminals) when unattended by pressing Ctrl-Alt-Del. At the end of the working day close down all the applications and log off/shutdown the workstation.
- Laptops must be locked away in a drawer or cabinet when the work area is unattended or at the end of the working day. Laptops must not be left at the site premises where the user is not sure about its security.
- User will be held responsible for handling information which is in his/her custody. It is the responsibility of each user to protect the privacy of the information they have access to and to take appropriate precautions in protecting the information.
- Electronic data and equipment shall not be treated differently from manual records and equipment, as they contain the same type of classified and/or personal information. Computers and all other equipment containing data should therefore be treated with a higher level of security when compared to paper-based resources.

- Computers and laptops must be protected by passwords, screensavers, and other security controls when they are left unattended for five minutes.
- While providing remote control of the computer for troubleshooting activities, users shall close and/or minimize sensitive documents and must be physically present at the system (as feasible).

6. Risk Management

Yubi Staff shall respect the confidentiality and privacy of customers whose records they access; observe any restrictions that apply to sensitive data; and abide by legislation, policies, procedures, and guidelines with respect to access, use or disclosure of information.

The unauthorized disclosure of data in any medium, except as required by an employee's job responsibilities is expressly forbidden, as is the access or use of any Data for one's own personal gain, or profit, or to satisfy one's personal curiosity or that of others.

7. Compliance

7.1 Responsibilities

- The Information Security Team is responsible for the development, implementation, and maintenance of the Clean Desk and Clear Screen Procedure.
- Company management is accountable for ensuring that the Clean Desk and Clear Screen Procedure and associated standards and guidelines are properly communicated and understood within their respective organizational units. Company management is also responsible for defining, approving, and implementing procedures in its organizational units and ensuring their consistency with the Clean Desk and Clear Screen Procedure and associated standards and guidelines.
- All individuals, groups, or organizations identified in the scope of the procedure are responsible for familiarizing themselves with the Clean Desk and Clear Screen Procedure and complying with its associated policies.

8. Policy Enforcement and Compliance

Compliance with the procedure is mandatory and Yubi department managers shall ensure continuous compliance monitoring within their department. Compliance with the statements of the procedure is a matter of periodic review.

Any breach of the procedure may constitute a security violation and gives Yubi the right to conduct disciplinary and / or legal action, up to and including termination of employment or business relationship.

Disciplinary action will be dependent upon the severity of the violation which will be determined by the investigations.

9. Waiver Criteria

The procedure is intended to address information security requirements. If needed, waivers shall be formally submitted to the Information Security Management, including justification and benefits attributed to the waiver by the CISO.

The policy waiver shall be granted for a period of four months initially and shall be reassessed thereafter and can be extended up to a period of three consecutive terms. No waiver shall be

provided for more than three consecutive terms on any of the policies.


10. Document Management

The document shall be maintained by the Information Security Team. Any requests for changes to the document must be provided to the CISO and will update the document, as appropriate. Until the document is updated, approved, and posted into the Yubi policies and procedures, the existing process must be followed, unless a deviation request has been granted.

Technological advances and changes in the business requirements will necessitate periodic revisions to documents. Therefore, the document may be updated to reflect changes or define new or improved requirements as and when required and in compliance with the Information Security Program Charter.

I hereby agree and accept the policy.

Employee Name : Harish B

Signature : 

Harish Baskaran (February 27, 2023, 8:27 GMT)

Date : 27-Feb-2023

ISMS Document

Email Procedure

Document Control ID: Yubi-ISPR-04.01

Issued Date: 19-10-22

Published Date: 19-10-22

Confidential and Proprietary Information of CredAvenue Private Limited ('Yubi'). Only expressly authorized for individuals under obligations of confidentiality with Yubi are permitted to review materials in this document. By reviewing these materials, you agree to not disclose these materials to any third party unless expressly authorized by CredAvenue Private Limited and to protect the materials as confidential and trade secret information. Any unauthorized review, retransmission, dissemination, or other use of these materials is strictly prohibited. If you are not authorized to review these materials, please return these materials (and any copies) from where they were obtained. All materials found herein are provided "AS IS" and without warranty of any kind.

DOCUMENT AND RECORD CONTROL

Revision Table

| Date | Version | Brief Description | Author |
|---------------|---------|----------------------------|-------------------|
| 03-October-21 | 0.1 | Email Procedure – Draft | Abinеш Athilingam |
| 04-October-21 | 1.0 | Email Procedure | Abinеш Athilingam |
| 17-October-22 | 1.1 | Updated to the Yubi Format | Devika Subbaiah |

Approval History

| Date | Version | Approval | Title |
|---------------|---------|----------|-------------------------|
| 04-October-21 | 1.0 | Approved | Chief Executive Officer |
| 19-October-22 | 1.1 | Approved | CISO |

Important Note: This document is intended solely for the use of the individual or entity to whom it is transmitted to, and others authorized to receive it. It may contain confidential or legally privileged information. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this document is strictly prohibited and may be unlawful. If you have received this document in error, please notify us immediately.

TABLE OF CONTENTS

| | |
|--|----------|
| Office of Responsibility | 3 |
| Purpose | 3 |
| Scope | 3 |
| Ownership and Responsibilities | 3 |
| General Guidelines and Approved Usage | 3 |
| Procedure | 4 |
| Creation of New Mail Accounts | 4 |
| Deactivation of E-Mail Account | 4 |
| Size of Mailbox and E-Mails | 4 |
| Virus Checking | 4 |
| Aliases and Lists | 5 |
| Automatic Email Forwarding | 5 |
| Password Policy Enforced | 5 |
| E-Mail Footer | 5 |
| Emails to Customers | 5 |
| Monitoring and Logging | 6 |
| Review | 6 |
| Spam and Junk Mail | 6 |
| Remote Access | 6 |
| Incident Handling and Data Protection | 6 |
| Backup, Archival and Retention | 6 |
| Procedure Disclaimer | 6 |
| Compliance | 6 |
| Responsibilities | 6 |
| Procedure Enforcement and Compliance | 7 |
| Waiver Criteria | 7 |
| Document Management | 7 |

1. Office of Responsibility

Chief Information Security Officer

2. Purpose

The purpose of the procedure is to describe the acceptable use of the CredAvenue Private Limited ('Yubi') email and related services, systems, and facilities. There will also be periodic review of the Procedure and, if necessary, amendment from time to time.

3. Scope

The procedure is intended to detail the rules of conduct for all Yubi employees, IT Administrator / Manager, users, auditors, contractors, consultants who use email and related services. The Procedure applies to the use, for the purpose of sending or receiving emails and attachments. Only authorized users of the Yubi systems are entitled to use email facilities. All members of the Yubi, who agree and abide by the Yubi regulations, are entitled to use computing facilities and email systems at all times.

4. Ownership and Responsibilities

Every user of an email system has a duty to ensure they practice appropriate and proper use and must understand their responsibilities in this regard. Yubi employees, IT Administrator / Manager, users, auditors, contractors, and consultants should be aware of the procedure and Yubi should ensure they abide by it.

5. General Guidelines and Approved Usage

- The e-mail systems are intended for use in the conduct of Yubi business. All e-mail messages will be considered as Yubi records and there must be no expectation of personal privacy.
- E-mail systems must be used primarily for business purposes only. No individual can use their personal email accounts for sending official mails or vice versa.
- Users will be responsible for effective usage of e-mail. Each user will be responsible for the contents of his / her message. All e-mails will be identified with a user's name or e-mail ID to allow for individual tracking.
- Individuals accessing the e-mail services of Yubi must not use or access an email account assigned to another individual to either send or receive messages.
- Attachments received from not trusted sources should not be opened.
- All emails must conclude with a signature file and contact information.

The Yubi main purpose in providing IT facilities for email is to support approved business activities of the Yubi. IT facilities provided by the Yubi for email should not be abused.

- Unauthorised/Unacceptable use of e-mail will include, but is not limited to: *
 - Transmitting or storing offensive material.
 - Compromising the security of information contained on Yubi computers by forwarding/sending Yubi mails containing sensitive information to external parties

(unauthorised recipients) without business justifications and/or applying adequate security controls.

- Soliciting for political, personal, religious or charitable causes or other commercial ventures outside the scope of the user's employment and the user's responsibilities to Yubi.
- "Spamming" sending unsolicited messages, promotions, sending or forwarding chain letters.
- 'Letter bombing' (re-sending the same e-mail repeatedly to one or more recipients).
- Creating, sending, receiving or storing materials that infringe the copyright or other intellectual property right of any third parties.
- Sending, transmitting or distributing proprietary information, data or other confidential Yubi information.
- Incidental and occasional personal use of the Yubi e-mail system will be permitted. However, information and messages stored in these systems will be treated in the same manner as business-related information and messages.
- Users must not create, or forward externally provided e-mail messages which may be considered to be harassment, or which may create a hostile work environment.

6. Procedure

6.1 Creation of New Mail Accounts

All members of Yubi will be assigned a Mailbox and Google Drive. The IT team will be responsible for creating user accounts on receipt of request (New hire intimation) from HR department.

All email users (including contractors and consultants) will sign an Email Acceptable Use agreement prior to using the e-mail facility.

6.2 Deactivation of E-Mail Account

The e-mail account of an employee leaving Yubi will be deactivated immediately on the last working day. IT team will receive email from the HR department, with all required details for de-activation, such as, Employee Name, Employee ID, date of release etc., along with the clearance checklist form.

7. Size of Mailbox and E-Mails

Google for business gives unlimited storage.

8. Virus Checking

- All email communication through email gateways shall be checked for malware.
- Email servers as well as all users' systems shall be installed and updated with latest version Crowd Strike software to monitor and quarantine malwares on a real time.
- Users shall follow certain strategies to avoid spread of malware; these include not opening executable attachments and scanning the messages/attachments.

9. Aliases and Lists

All Yubi employees, System Administrator / Manager, users, contractors, will be allocated email aliases based on their initials and surname. Email alias duplications are possible, so it is sometimes not possible to offer the exact email alias to users. Specific email aliases can be requested for individual, or group use if there is legitimate requirement. Email lists can also be created. Generally, individuals requesting a list will be responsible for the ownership and management of the list.

10. Automatic Email Forwarding

Automatic forwarding or redirection of email to other mail domains is permitted, when forwarded manually; it should be done only to legitimate (Yubi employees, System Administrator / Manager, users, auditors, contractors, consultants and third parties) users of the Yubi with proper approval.

11. Password Policy Enforced

Password policy is enforced for the email through Google Authenticator

- Minimum Password Length = 10 characters (that should include lower case letter, upper case letter and Number (0-9)).
- Maximum Password Age = 100 days.
- Password expiration = 60 days.
- Maximum number of password reuse/history will be at 5.
- Maximum Password age should be at 60days.
- Account lockout for incorrect attempts should be 5 retries.
- For Lock out – Reset should be done by Account Administrators.

12. E-Mail Footer

- All e-mails will carry an automatic standard footer banner. The banner will indicate that:
 - The mail is intended for the use of the recipient to whom it is addressed.
 - The mail shall not be acted upon and destroyed promptly if a person, to whom it is not intended, receives it.
 - Opinions, conclusions, and other information in the message that do not relate to the official role of the sender shall be understood as neither given nor endorsed by Yubi.

13. Emails to Customers

- Yubi shall never ask for personal information from customers through email.
- Yubi shall never provide clickable links in an email to customers.

14. Monitoring and Logging

The Email Usage activity log can be retrieved to identify any non-compliant activity. Email alert to the Super admin is set for the activities like Device Compromise Update, suspicious mobile activity.

In the event of non-compliance need the IT Team can retrieve basis logs.

14.1 Review

The Auditors from Information System Audit will conduct periodic and regular reviews to ensure that access to e-mail facilities have been granted to authorized users.

14.2 Spam and Junk Mail

Spam can be defined as “the mass electronic distribution of unsolicited email to individual email accounts”. Junk mail is usually a result of spamming. In reality spam and junk mail are regarded as interlinked problems.

14.3 Remote Access

As part of the Corporate Messaging Environment all the employees of Yubi are provided access to email by remote means. The features listed below have been enabled for access to corporate emails from anywhere (at home or while travelling).

Web Access – Access email over the web with a unified URL (<https://mail.XXXX.com>) with unique username and password for sign in.

RPC over HTTPS – This is access email over the internet using outlook client without using VPN and this service available only for Managers and above.

14.4 Incident Handling and Data Protection

The Yubi shall investigate complaints received from both internal and external sources, about any unacceptable use of email. The logs should be only kept for limited periods of time so the prompt reporting of any incidents which require investigation is recommended. In such cases Yubi will act immediately with the priority of preventing any possible continuation of the incident.

14.5 Backup, Archival and Retention

The service provider takes care of the Backup, Archival and Retention.

14.6 Procedure Disclaimer

If any user is found to have breached the procedure, they may be subjected to Yubi disciplinary procedure. If a criminal offence is committed action may be taken to assist in the prosecution of the offender(s) and are subjected to central jurisdictions.

15. Compliance

15.1 Responsibilities

- The Information Security Team is responsible for the development, implementation, and maintenance of the Email Procedure.
- Company management is accountable for ensuring that the Email Procedure and associated standards and guidelines are properly communicated and understood within their respective organizational units. Company management is also responsible for defining, approving, and implementing procedures in its organizational units and ensuring their consistency with the Email Procedure and associated standards and guidelines.

- All individuals, groups, or organizations identified in the scope of the procedure are responsible for familiarizing themselves with the Email Procedure and complying with its associated policies.

16. Procedure Enforcement and Compliance

Compliance with the procedure is mandatory and Yubi department managers shall ensure continuous compliance monitoring within their department. Compliance with the statements of the procedure is a matter of periodic review.

Any breach of the procedure may constitute a security violation and gives Yubi the right to conduct disciplinary and / or legal action, up to and including termination of employment or business relationship.

Disciplinary action will be dependent upon the severity of the violation which will be determined by the investigations.

17. Waiver Criteria

The procedure is intended to address information security requirements. If needed, waivers shall be formally submitted to the Information Security Management, including justification and benefits attributed to the waiver by the CISO.

The procedure waiver shall be granted for a period of four months initially and shall be reassessed thereafter and can be extended up to a period of three consecutive terms. No waiver shall be provided for more than three consecutive terms on any of the policies.


18. Document Management

The document shall be maintained by the Information Security Team. Any requests for changes to the document must be provided to the CISO and will update the document, as appropriate. Until the document is updated, approved, and posted into the Yubi policies and procedures, the existing process must be followed, unless a deviation request has been granted.

Technological advances and changes in the business requirements will necessitate periodic revisions to documents. Therefore, the document may be updated to reflect changes or define new or improved requirements as and when required and in compliance with the Information Security Program Charter.

I hereby agree and accept the policy.

Employee Name : Harish B

Signature : 

Harish Baskaran (February 27, 2023, 8:27 GMT)

Date : 27-Feb-2023

Nominee Declaration Form


I hereby confirm that in case of any unforeseen event, the below mentioned nominees will be receiving the benefits in my absence. (Group Term Insurance / Gratuity / Smile and Tears Policy / ESOPs [If applicable])

(E.g., Father, Mother, Spouse, Son, Daughter/ Adopted Parents/ Adopted Children) can be added as the nominees.

Please provide the below details:

| S. No | Nominee/Appointee Name | Relationship | Claim Percentage |
|-------|---|--------------|------------------|
| 1. | Aswathi Rajasree I Block N Flat-071 SBIOA Unity Enclave, Mambakkam Chennai - 600127 | Wife | 100 |

Employee Name : Harish B

Signature : 

Harish Baskaran (February 27, 2023, 9:27 GMT)

Date : 27-Feb-2023

| | |
|---------------|--------------------------------------|
| CONTRACT NAME | Employment Agreement (Merged) |
| CONTRACT ID | ac262e05-59a8-4670-9786-e913f7d2d115 |
| STATUS | Executed |

CONTRACT HISTORY



SIGNED

Signed by **Abhishek Mehrotra** (abhishek.mehrotra@go-yubi.com).

27 February, 2023 09:26:07

UTC

IP: 0.0.0.0

Location unavailable



SENT

Sent for Signature to **Harish Baskaran** (harish.baskaran@go-yubi.com) by **Kavya Sakthivel** (kavya.sakthivel@go-yubi.com).

27 February, 2023 09:26:09

UTC



SIGNED

Signed by **Harish Baskaran** (harish.baskaran@go-yubi.com).

27 February, 2023 09:27:20

UTC

IP: 134.238.236.53

Location unavailable



EXECUTED

This document has been signed and executed by all parties.