Dar Credit & Capital Ltd.

...we make life simple

INFORMATION TECHNOLOGY POLICY

In fulfilling our business mission, we use a wide variety of information technologies (IT) to grow our business. The Information Technology Policy provides all employees (including part-time, trainee and temporary employees) with guidelines for the proper use of all the computer's hardware and software, Laptop, UPS, Data cards, e-mail, Switch, Internet services, Business Software and other information technology equipment's. It also provides a framework for purchasing all Servers, Network equipment's, Desktop and Laptop computers, Telephones, Data cards, and other technology equipment and all kinds of Software for our Head office/Branch office or our business use. Further, all IT equipment's and software which we purchased is the property of Dar Credit & Capital Limited (DCCL).

All computers, software and peripheral devices which are attached to or used with a personal/company computer or laptop must be ordered only after consultation with the IT Department & should have written approval from higher management.

Purchasing Policy:

In order to coordinate and standardize on technology equipment (computer's hardware and software, Laptop, UPS, Data cards, e-mail, Switch, Internet service and other information technology equipment's) and software purchases in a uniform and planned way, the following purchase procedure is to be used:

1. Requisition is prepared by the employee and approved as appropriate by the /Director/Chairman. Justification (business purpose) for the purchase must be indicated on the requisition.
2. IT Dept. collects at list three (03) quotations from different venders.
3. To be verified license compliance issues for software purchases.
4. Respective IT member meet with the venders & talk with them regarding the Quality, after sale Service & Support, Warrant, Delivery, Price & Advance related issues.
5. IT Member shall give signature on every quotation.
6. One comparison sheet is prepared (Including Price, Quality, Support and Warrant) by the concerned IT member.

7. The Comparison sheet & necessary documents (Service & Support, Warrant, License, Price list, Delivery etc.) are submitted by the IT member to the Director/ Chairman for the approval. [Before approval, shall talk with Accounts Dept. & must be made aware for fund requirement].

8. After receiving the approval, one Work order/Purchase order to be made by the IT member & placed it to the selected vendor.

9. After receiving the item from the vender, the IT dept. should verify the quantity, the quality of the item, the warranty status and the licensing issue.

10. If the point no -9 is satisfied by the IT dept., then only the IT Dept. receives the item form the vender

Access and Use

All employees share the Information Technology facilities at Dar Credit & Capital Limited (DCCL) These facilities are provided to employees for the purpose of conducting Company business. The Company does permit a limited amount of personal use of these facilities, including computers, Laptops, printers, e-mail and Internet/Data Card access. However, these facilities must be used responsibly by everyone, since misuse by even a few individuals has the potential to negatively impact productivity, disrupt company business and interfere with the work or rights of others. Therefore, all employees are expected to exercise responsible and ethical behavior when using the Company's Information Technology facilities. Any action that may expose the Company to risks of unauthorized access to data, disclosure of information, legal liability, or potential system failure is prohibited and may result in disciplinary action up to and including termination of employment and/or criminal prosecution.

The following topics are covered within this policy and referred policies:

• General Information Technology Usage Policies;

• Software Licensing Policy;

• Hardware Policy;

• E-mail Usage Policy;

• Internet and Intranet Usage Policy.

General Information Technology Usage Policies:

Users of DCCL accept the following specific responsibilities:

1. Access to the information technologies is intended for the pursuit of DCCL's business goals and its administrative functions and shall not be used for personal commercial reasons or any other unauthorized use.

2. A computer username and password is intended for the exclusive use of the person to whom it is issued. Sharing of usernames and passwords amongst unauthorized persons is strongly discouraged, and all responsibilities must be borne by the person to whom a username is initially issued.

DCCL requires that all users choose secure passwords with a minimum of six (6) characters. Avoid words found in the dictionary and personal information. Include at least one numeric character.

3. Users shall not attempt unauthorized access to computing resources either within the company or outside.

4. Users shall use all systems in compliance with proprietary rights and be aware that, in addition to disciplinary action, as described in paragraph 17 below, any violation of proprietary rights will result in the liability of the user.

5. Users shall not use information technology systems for any unauthorized or illegal purpose, such as, but not limited to, the destruction or alteration of data owned by the company or third parties, the interference with restricted access to the information technology systems, the disruption of the systems, the attempt to discover or alter passwords or to subvert security systems, or the transmission or retrieval of offensive material.

6. Users shall protect computer equipment from theft. It is prohibited to move fixed computer equipment out of an area to which it was assigned, without proper authorization.

7. Users shall protect confidential or sensitive information stored on their hard disk by having adequate password control, which must be renewed regularly.

8. Users shall protect DCCL's data from loss. If data is not kept on a network server, which is backed up, then it is the responsibility of individual users to ensure that data is backed up on a regular schedule. The location of back-ups shall be agreed upon with, and known to department management.

9. Users shall not remove company-owned software from the premises other than as part of a computing device made available by Company, without prior approval.

10. Users shall not send electronic communications that appear as though they were sent by someone else, without their express consent.

11. Users shall not send electronic junk mail, chain letters, jokes and alike, and messages of content that are considered offensive or disruptive such as, but not limited to, obscene or racial, ethnic, sexual or gender specific harassing language or images.

12. All approved notices of a personal nature should only be posted on the bulletin boards designated for that purpose.

13. Users shall not use, install, load or download any unlicensed commercial software or any unauthorized software. Non-commercial or personal commercial software must not be loaded unless approved by the information technology management.

14. Users shall not ask for or make any illegal copy of licensed software.

15. Purchase and disposition of hardware and software shall be coordinated with the information technology management.

16. All users shall report any unauthorized access attempts or other improper usage of DCCL's computers, networks or other information processing equipment. If you observe, or have reported to you, a security or abuse problem with any DCCL computer or network facilities, including violation of this policy, you are encouraged to notify either the information technology management or other appropriate administrator.

17. Any use of DCCL's information technologies that is contrary to this policy could lead to disciplinary measures up to and including termination of employment and legal action. Some violations may also constitute criminal offences, as outlined in local/municipal, state/provincial or federal laws. DCCL will carry out its responsibility to report such violations to the appropriate authorities.

Software Licensing Policy:

1. Installing Software –DCCL's staff are NOT authorized to install any software, programs, batch files, or screen savers on DCCL's computer equipment. It is the responsibility of the IT Department to complete these tasks.

2. Unauthorized Downloadable Software – The use of unauthorized downloadable software is prohibited. Downloadable software such as freeware, shareware, program demos, surveys, advertising, training, Internet browsers, copyrighted data, fonts, personal digital images,

graphics and personal photos should not be downloaded without prior approval by the Management and the involvement of the IT staff

3. Software Licensing Compliance –Violation of any software licensing agreement, copyright, or other intellectual property rights of third parties is strictly prohibited. This includes, but is not limited to, computer software/data or related manuals and materials. Contact the IT Department for more information about software licensing agreements. Users also are required to conform with the terms and conditions of all license agreements.

4. Software programmes, applications, or '.exe files', must only be stored on a user's local hard disk drive.

5. Chat Rooms /News Groups/Instant Messaging – Only those employees who are authorized to speak to the media, to analysts, or at public gatherings on behalf of the company may speak (write) in/ at any Internet chat room / news group or on Instant Messaging. This can occur only after going through the normal Head of the Dept. review and approval process within the Department. Instant messaging/Chat rooms and the like are expressly prohibited to all employees unless specifically authorized by the employee's HOD.

6. Privacy – Management has the right to inspect and disclose to appropriate people any and all files and /or messages stored on any DCCL's computer, including e-mail files.

7. Viruses – The IT network or any TCHD computer resource shall not be used to download or distribute pirated software or data, or to propagate any virus or variant thereof.

8. Virus Scan –ALL disks, removable media, and drives from any outside source MUST be scanned for viruses prior to opening the contents on the disk/removable media/drives.

Hardware Policy:

1. Moving Computers –No users are permitted to remove any DCCL's computer equipment, components or software from the company premises without prior authorization from and involvement of the IT staff, excluding properly checked out laptops and LCD projectors.

2. Installing and Removing Hardware - Users are not authorized to attach/detach or install/uninstall any computer components without authorization from their Dept. Head and involvement of IT staff. This includes keyboard, mouse, printer, modem, monitor, internal boards, or other components. The IT Department is responsible for assigning computer components to specific computers.
3. Storing Data – All data must be stored on designated servers, not on local hard drives when that option exists. Data on the servers are backed-up nightly, thus protecting the user from loss of data should a computer malfunction. Data storage space on the servers is limited. Therefore, users with the need for an extraordinary amount of data storage should notify their Dept. Head who will then work with the IT staff to meet the user's needs. If portable media containing electronic protected health information is generated, the user must take the responsibility to store the media in a secured, locked location and dispose of the media per the media disposal guidelines when no longer needed.

4. Working From Home – Processing of the Company business on a home computer is permissible as long as copyright, confidentiality, or public information laws are not violated. Staff working from home must have updated virus protection software on their computer. IT Dept. will supply virus protection software and other standardized software to staff working from home upon authorization from their Dept. Head.

5. Acquiring and Disposing of Computer Hardware – The purchase of any computer hardware or the disposal of old computer hardware is done only with the approval of the DIRECTOR/CHAIRMAN and involvement of IT staff. Please check with IT staff on proper disposal of removable media (CDs or floppy disks) containing confidential information.

E-mail Usage Policy:

1. DCCL provides access to employees for using email under the company's domain name. The employees need to ensure that no external party send mails from such IDs.

2. The mail ids are subject to tenure of server and will be withdrawn in case the employee leaves the services.

Internet Usage Policy:

Access and Use

1. DCCL provides access to the internet through its server for the use of its employees who require it in order to fulfill their functions. Information technology management authorizes access.

2. While using internet, employees must apply the following principles:

   - Maintain DCCL's reputation;
   - Utilize the Internet as a tool for continuous improvement of efficiency and performance;
   - Ensure and maintain a high level of professionalism in keeping with DCCL's Code of Ethics.

Rules of Utilization

When using DCCL's access to the Internet, whether during or outside working hours, the following rules must be followed:

1. Internet access may be used only for DCCL's business purposes.

2. Internet usage must be able to survive public scrutiny and/or disclosure. Users must avoid accessing sites that might in any way bring discredit on DCCL such as those sites that carry offensive material.

3. Accessing or disseminating information that is illegal, defamatory, abusive, racially offensive, and/or adult-oriented is strictly prohibited.

4. Fraudulent, harassing or obscene messages and/or material are not to be sent, printed, requested, downloaded or stored; chain letters and other forms of mass mailings are also prohibited.

5. Users must not engage in personal commercial activities on the Internet, including offering merchandise for sale or ordering services or merchandise from on-line vendors.

6. It is the responsibility of each user to recognize and respect the intellectual property of others and to comply with all applicable laws and regulations and the legal protection provided by patents,

trademarks, copyrights and licenses with respect to both programs and data downloaded from the Internet.

7. It is the responsibility of each user to respect and value the rights and privacy of all, to recognize and respect the diversity of the population and opinions of other Internet users, to behave ethically and to comply with legal restrictions regarding the use of information resources.

8. It is the responsibility of each user not to engage in any activity that would compromise the security of any host computer or circumvent any computer security measures imposed. In this context, it is prohibited to obtain passwords belonging to others, give out passwords, or to represent oneself as another user, or to attempt to ascertain security access codes.

9. All software, freeware, patches or other form of application must be reviewed by the information technology management for technical approval before downloading to reduce the risk of conflicts with other standard software products, operating systems and LAN products. Authorized application should be installed by qualified IT personnel.

10. Downloads from the Internet are potential sources of computer viruses. All files originating must be scanned for viruses before use.

11. Internet access to streaming media such as online television and /or online radio is restricted to business purposes only and must be authorized by the information technology management to adequately monitor network loads.

12. Employees should limit their communications to topics in which they have a professional responsibility and expertise. All communications should be regarded as "on the record" and attributable to the employee who posted or sent the information.

13. proprietary information or documents must not be sent over the Internet unless they are transmitted in a fully secured manner. Legally privileged information such as contracts, opinions, etc., should not be transmitted, under any circumstances.

14. Generally, each user must keep in mind that utilizing the Internet through DCCL's gateway may have legal implications and consequences. When engaging in activities on behalf of DCCL, online, individual users must exercise extreme caution as any of these activities have legal such as trading, selling, buying, marketing, advertising, etc., on the Internet or on-line, individual users must exercise extreme caution as any of these activities have legal consequences and may create legal consequences and may create legal obligations for the company. Before proceeding, proper authorizations must be obtained. If in doubt, advice may be sought from the appropriate Department.

15. Any inappropriate use or one that is contrary to this policy could lead to disciplinary measures up to and including termination of employment and legal action. Some violations may constitute criminal offences, as outlined in local/municipal, state/provincial or federal laws. Domtar will carry out its responsibility to report such violations to the appropriate authorities.

Backup Management/Backup Policy

Backup reduces risk of data loss and restores data quickly when called upon. Backup service enables faster recovery from server failures, improper configuration caused by Human errors like inadvertent deletions or overweight of files, directories or websites and other important data. It mitigates hacker attacks and restores affected sites.

Backup service includes:

1. Data shall be backed up in accordance with the requirements and specifications provided by the user, subject to the Company's applicable backup procedures and policies.
2. The Company's database is backed up daily using Amazon Web Services (AWS), a widely adopted cloud computing platform. These backups support data protection and enable recovery in the event of data loss, system failure, or other disruptive incidents.

Qbent Customer Support

- Help Desk (Online / Telephonic / Email/ WhatsApp Group) support – Prompt and responsive helpdesk support.
- Service Availability – Availability of support services 24 hours a day 7 days a week to help troubleshoot problems.

  Availability of logging your calls from single point of contact via any modes of communication (phone, Email, WhatsApp Group).

Data Security

1. The Company does not maintain a centralized repository for storing data generated by employees on their respective desktop computers and laptops. Accordingly, each system owner shall be responsible for regularly backing up the data generated and maintained on their respective systems to the designated **"D" drive**.

Additionally, the **Secretarial Compliance Team** shall store its data in the designated **"Data Sharing"** folder available on the systems used by the team.

2. The users should avoid keeping their data in "C" drive or on desktop or in "my documents". The best way to keep the data safe (as much as possible) to keep them in "D" or "E" drive in different directories. Pl. try to keep "C" drive undisturbed as much as possible. "C" drive is most vulnerable as it contains the operating system.

3. To avoid corruption of file (particularly Excel) please don't open big sizes excel files more than one at a time.

4. Do not try to open more than 2-3 applications at a time to avoid data corruption & avoid slow performance of the system.

System Usage Policy

1. Restrict physical access to PCs and Laptops to only authorized personnel.

2. Secure PCs (screen lock or logout) prior to leaving area to prevent unauthorized access.

3. Ensure PCs and peripherals are used for authorized business purposes only.

4. Keep food and drink away from PCs and Laptops in order to avoid accidental spills.

5. Don't give out your password to anyone, including the system administrator. It's your own and should be guarded carefully.

6. Don't install any extra software on your system from external sources such as the Internet, or your personal CDs and pen drives. This could have malicious code that could destroy data on your system, or even spread it to other systems on the network.

7. If you find a problem with your PC, printer or with any computer peripheral, don't try to fix it yourself. Call the IT support staff and lodge a complaint.

8. Shut down your system properly when you're leaving for the day to save power.

9. Don't store your personal data such as family photos, songs or videos in your office PC or in Laptop.

10. In case you need to share files with somebody else on the network, then send them by e-mail only. For this try to avoid pen drive as much as possible.

11. Don't leave or keep critical documents in the "C" drive or in the "my documents" or in the "desktop" of a PC. Always try to keep these files in separate folder in "D" or "E" drive.

12. Avoid keeping any data in the "C" drive.

13. NO PERSONAL computer and/or Laptop can be plugged into the company Network system or attached to the wireless system without inspection by the IT Department first and approved.

Network Usage Policy

1. In case the system is not able to access the network, don't try to tamper with the network settings and cables. Call the IT support staff instead.

2. Don't switch off the network equipment's like network switches, modem, WAP etc.

3. Don't send unnecessary traffic on the network, such as chain mails. Some viruses send huge traffic in the network causing a network choking.

4. Don't try to fix up any static IP to your PC without the permission of the support IT staff. System had been set to allocate dynamic IP to all PCs.

5. Disruptive behavior such as introducing viruses or intentionally destroying or modifying files on the network is strictly prohibited.

6. No Laptop or any wireless capable device which do not belong to company will not be connected to company wireless.

7. Wireless AP or any wireless device password will not be shared with anybody under any circumstances.

Anti-Virus Policy

1. Always run the corporate standard, supported anti-virus software available from the IT department. This antivirus is loaded either locally or remotely by the IT support staff to the PCs. This is centrally monitored, updated and controlled.

2. Don't try to uninstall or tamper with the antivirus software installed in the PCs.

3. Don't try to install any other un-authorized antivirus unless otherwise permitted by the IT department.

4. NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.

5. Delete spam, chain, and other junk e-mail without forwarding.

6. Never download files from unknown or suspicious sources.

7. Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.

8. Always scan a pen drive or external HDD from any source for viruses before using it.

9. Try avoiding using pen drive.

10. New viruses are discovered almost every day. Periodically check the Anti-Virus update date in the installed antivirus in your PC. If the update date is at least 7 days old please inform IT support team.

Internet Usage Policy

1. Any personal use of the network for commercial or illegal activity is strictly prohibited.
2. E-mail and file transfers are to be for business use only by authorized users.
3. Use of another employee's account for access of Internet is strictly prohibited.
4. Confidential information is not to be transmitted over the Internet without proper permission.
5. All downloaded files or applications are to be scanned for viruses before being saved on the PCs.
6. Access to non-business related, obscene or offensive sites or any kind of social or shopping sites is strictly prohibited.
7. Game playing is strictly prohibited.
8. Use of public Instant Messengers such as Yahoo, **Skype** and MSN is strictly prohibited (or not permitted). **Chairman however can allow use under his direction against specific application.**
9. Don't download unnecessary software, songs or videos. These take up significant Internet bandwidth.
10. Installing download accelerators is not allowed.
11. Don't visit objectionable Web Sites containing bad language and pornography.
12. Chatting over the Internet is not allowed.
13. Any attempt of defeating or attempting to defeat security restrictions on company systems and applications is highly objectionable and punishable offense.

Mail Usage Policy

1. **Sending chain mails is highly prohibited.**

2. **Sending any mail on different subject under the same heading is not allowed.**

2. Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages is punishable offense.

3. Sending, receiving, or accessing pornographic materials is punishable.

4. Causing congestion, disruption, disablement, alteration, or impairment of Company networks or systems is also punishable.

5. Avoid sending jokes to huge mailing lists.
6. If you get a mail that's been forwarded to a long list, don't hit the Reply All button if you only need to inform the sender.

7. Avoid sending huge attachments in e-mail, unless it's official.

8. Don't reply to any spam mail, even if it gives instructions to do so. This will actually confirm your presence to the spammer, and you could be spammed even more.

9. Be wary of opening e-mail attachments, unless you're sure that it's from a reliable source, and that you were expecting it. If necessary, call up the sender to check.

10. Employees must be aware that the electronic mail messages sent and received using Company equipment are not private and are subject to viewing, downloading, inspection, release, and archiving by Company officials at all times.

11. Mail ID creation, deletion and blocking is under sole discretion of IT Department**, based on the direction of Chairman.**

12. IT Department has to right to access any computers and control in this office and branch office, at any time sole discretion.

Software Usage Policy

1. The Company has licensed the use of certain commercial software application programs for business purposes (like MS Office, MS Windows, Antivirus, SQL Database, etc.) Third parties retain the ownership and distribution rights to such software. No employee may create, use, or distribute copies of such software that are not in compliance with the license agreements for the software. Violation of this policy can lead to disciplinary action, up to and including dismissal.

2. It is to be noted that preserving the cracked software, used for cracking any of the design or any other software is also not permitted and is illegal.

Business Software (Vijay & Rise Money) Usage Policy

1. Some masters (Branch Master, Loan Related Master, Loan Product Related Master, and Purpose/Sub Purpose Related Master) will be created by the IT functional core team members only. The request for the same has to be sent via prescribed format only and approved by the high level of Management (Director/Chairman). Opening of a new master record will be totally on the discretion of functional lead of that module and the process owner. No master will be created or changed over phone.

2. Any change or creation of new module, new reports, logic change of any existing modules, add or modify any column or change logic of any existing reports will be sent via prescribed format only and approved by the high level of Management only.

3. User Acceptance Test (UAT) should be done by the submitter on the test server. If the test server shown the satisfactory result and fulfill the entire requirement which have been submitted by the submitter earlier, the IT Dept. shall send the request to software vendor for shifting/apply the new logic into the main server. No data will be created or changed over phone.

4. HR Dept. shall add and create user ID for all new employees. Transfer, Promotion, Demotion, Active/ Inactive user ID or employee should be done from HR Dept.

5. Assign role, change role, assign branch, add branches, change branch should be done by HR. Dept.

6. Create new role or change any activity of existing role should be done by the IT Dept. after receiving the approval from top Management.

7. Modification of existing report, new development etc. is the sole discretion of IT HOD and functional lead of that module.

8. Monthly Financial period closing date to be decided by management. But once the financial period of the previous month is closed it will not be opened without the written order from top management and during that period only some designated user's will be allowed to make entry in the system in back date.

9. It is always advisable to use the standard reports for any kind of audit purpose. When the standard reports are inadequate to suffice the purpose, then only customized reports can be extended for these purpose after thorough checking by the functional team members. IT does not give the guarantee of authenticity of any customized report or program built inside and run on backup database by internal IT team.

10. Loan Application should be sanctioned by Credit Bureau data and as per the logic which have been decided by the top Management.
11. Head of Operation and AGM Opps has the full power/access to approve/sanction cancel loan application.

12. Loan disbursement shall be done at HO Credit Team.

13. The posting Installment Collection shall be done at Branch by the Branch Manager.

14. Selected users will access Mobile Application.

15. Through Mobile Application selected users will be disbursed loan and collected installment amount from center.

16. Only some designated users will be allowed to make entry in the system for Insurance settlement and loan write off. But for both cases pre approval shall be needed from the top Management.

17. For fund transfer or receipt, only some designated users will be allowed to make entry in the system.

Maker Checker Framework

To reduce operational risk, eliminate single-point data manipulation, and ensure data integrity across all systems, DCCL adopts a strict Maker-Checker protocol across all core business applications (including Vijay & Rise Money platforms):

- **Dual Control Enforcement:** Every critical transaction—including loan creation, disbursement approvals, fee waivers, loan write-offs, and ledger journal entries—must involve at least the following:
  - **Maker:** The authorized user who initiates or inputs the transaction/data into the system (Branch Officials);
  - **Checker:** An independent authorized user (or higher-level supervisor) who reviews, verifies, and approves the transaction before system commitment (Senior personnel at the Head Office of the Company).

Digital Signature Certificates (DSC), Mobile Financial Services, & Social Media

Pursuant to Chapter IV (Paragraphs 31, 33, and 34) of the relevant RBI Directions, the following standards shall be adhered to:

Digital Signature Certificates (DSC)

- DSCs issued to authorized company officers (for regulatory submissions, banking operations, or legal contracts) must be stored in secure cryptographic hardware tokens.

- Sharing DSC passwords or handing over tokens to unauthorized personnel is strictly prohibited. An inventory register of all active DSCs and their custodians shall be maintained by the IT Department.

Mobile Financial Services

- All mobile applications utilized for customer onboarding, verification of documents like KYC, collection of installments must enforce strong end-to-end encryption.

Social Media Governance

- Official social media accounts of DCCL shall be managed exclusively by authorized personnel

under designated supervisory review.

- Employees shall not disclose confidential, proprietary, or sensitive company information on any public platform. Employees shall also refrain from making unauthorized official statements or comments on behalf of DCCL through personal or official email IDs or any other communication channels.

System generated reports for Senior Management

The IT system shall automatically generate periodic reports summarizing financial position including operating and non-operating revenues and expenses, cost benefit analysis of segments / verticals, and cost of funds to enable continuous oversight by Board of Directors and Senior Management of the Company.

Standard Operating Procedure (SOP) for Application User Access Management

1. The relevant user places a requisition to his Head of Department for authorization of access to any particular transaction/ Module/ Reports through prescribed format. The Head of the Department approves the same and forwards the requisition to the head of the IT department.
2. The head of the department decides that authorization for a particular transaction/ Module/ Reports are required by the user to perform a specific activity; accordingly, he forwards a mail and the filled up the format (Signature is required) to the relevant functional head of the IT department.

3. If considered acceptable, the relevant functional head forwards the said requisition to the head of the IT department. If not, he communicates the same to the HOD & decides on an alternative course of action or gets re-confirmation of the same course of action from the HOD.

4. The IT head gives authorization to the user as per requisition made.

5. IT head has the full authority to revoke authorization from any user in case of misuse or using against company norms.

Change Management Procedure in Vijay & Rise Money Software:

1. Change Management may be triggered by any user or IT core team member or any Dept. Head. Change requests are accepted via prescribed format or in some cases via mail communication.

2. If any change is required, it is sole responsibility of the concerned IT core team member to arrange the changes (depending on the feasibility) and test in testing server.

3. This may be tested by core team member and he may get it tested by the user or Dept. head.

4. After the satisfactory testing the change will be transported to the main server.

5. In case of minor changes IT core team member does not need any permission from HOD. In case configuration changes, new development, new report or major changes he needs permission from HOD to carry out the specific task and transport.

6. If any financial cost for deployment the requirement, shall take the approval from **any one Director.**

Robust Information Security and Cybersecurity controls

The Company utilizes Amazon Web Services (AWS) as its cloud infrastructure platform, through which adequate information security and cybersecurity controls are maintained. The Company shall ensure effective oversight and review of such controls to maintain the security and integrity of its information assets and IT systems.

Automated Regulatory Returns Filing with RBI

DCCL's software and database shall possess inherent capability and data integrity to compile and generate all mandatory regulatory returns required by the RBI (including return filings under the CIMS platform).

Business Continuity Plan (BCP)

Business Continuity Plan: DCCL has established a comprehensive BCP policy detailing Key Business Operations, Products and Future Growth Plan for the next three years, which shall be presented to the Board of Directors for review and approval at least once every year.

EMPLOYEE POLICY ACKNOWLEDGMENT INFORMATION TECHNOLOGY (IT) POLICY

I acknowledge that I have read the Information Technology Policy (IT). I understand that the information contained in this policy supersedes any written or verbal policies I may have received in the past.

My signature below indicates that I have familiarized myself with the information contained in the policy and that I will seek verification or clarification where necessary.

I understand that the information contained in the policy is subject to change as situations warrant. Further, I understand that changes in policy may be communicated verbally, in writing, or in an automated form. I accept full responsibility for keeping informed of the policy and practices in place at a given point in time, as well as for any changes thereto.

I understand that, as an employee of DCCL, if I fail to meet these standards, I will be subject to appropriate disciplinary action up to and including dismissal. If I have questions regarding this policy, I should discuss them with my supervisor/manager, Departmental Head, or Human Resources Manager.

I understand that this policy, and the related practices and procedures contained in the policy do not constitute any form of contractual or legal employment agreement between the company and me.

_____
Employee's Name (IN UPPER CASE)

_____ _____
Employee's Signature Date Date

Dar Credit & Capital Ltd.

...we make life simple

BUSINESS CONTINUITY PLAN

CIN: L65999WB1994PLC064438

Regd. Office: Business Tower, 206 AJC Bose Road 6th Floor, Unit No. 6B, Kolkata – 700017;

Phone: 033 40646495; Website: www.darcredit.com, Email- info@darcredit.com

1. Introduction

The Reserve Bank of India through its Master Direction **RBI (NBFC – Cybersecurity, Technology: Risk, Resilience and Assurance Framework) Directions, 2026** dated July 31, 2026 (as amended from time to time) provided guidelines for the Information Technology Framework for the NBFC sector. The objective of these guidelines is to ensure safety, security, and process efficiency within NBFCs. To meet these objectives, **Dar Credit & Capital Limited** ("**the Company/ DCCL**") has developed this Business Continuity Plan (BCP) to ensure operational resilience and minimize disruptions caused by unforeseen events.

2. Purpose and Scope

This BCP applies to all functions and operations of DCCL, including income generation, client services and reputation protection. It aligns with the company's IT policy to ensure clarity and comprehensive protection.

3. Objectives:

The objectives of DCCL's BCP are as follows:

- Manage and control identified risks.
- Protect Customer Interests and Maintain Data Integrity.
- Protect Reputation and Stakeholder Confidence.
- Prioritize recovery of critical business data within predetermined timeframes.

4. Organization Profile

Dar Credit & Capital Limited is a Listed Non-Banking Financial Company (NBFC) incorporated in West Bengal under the Companies Act, 1956. The Company holds an NBFC license from the Reserve Bank of India (RBI), and that it was established in 1994. Its registered office is in Kolkata, West Bengal, with a regional office in Jaipur, Rajasthan.

The Company was founded by Mr. Ramesh Kumar Vijay, who is a first-class Commerce graduate, Chartered Accountant and qualified Company Secretary. DCCL's stated business focus is to provide credit to customer segments that may have limited access to conventional banking channels.

5. Business Activities and Customer Segments

5.1 Municipal Employee Personal Loans

DCCL provides personal loans primarily to permanent municipal employees, including sanitation workers and other Group D employees. Arrangements with participating municipalities allow instalments to be deducted from employees' salaries and remitted to the Company on the relevant due dates. The product is described as addressing credit-access barriers faced by underserved employee groups and is mainly concentrated in Rajasthan, Madhya Pradesh and parts of Gujarat.

5.2 MSME and Small-Business Lending

The Company offers both secured and unsecured MSME loans. Its target customers include small shopkeepers, vendors, retailers, wholesalers and other entrepreneurs in rural and semi-urban markets. The main focus is financing the businesses that may lack conventional collateral, as well as mortgage-backed business loans where property security is available. The source document identifies West Bengal as a key market for this product. This product is mainly concentrated in West Bengal, Bihar, Jharkhand and Rajasthan.

5.3 Livelihood and Financial Inclusion

DCCL states that it supports livelihood promotion among low-income rural and semi-urban households through livelihood-related and microfinance services. Its stated objective is to promote sustainable livelihoods among population groups that are underserved by formal banking institutions. The Company follows applicable NBFC guidelines issued by the RBI from time to time.

6. Customer Base, Experience and Institutional Relationships

Dar Credit & Capital Ltd have more than 32 years of industry experience and reports approx. 25,000 active customers as at September 30, 2026, with assets under management (AUM) of ₹260.19 crore and employee strength of 300+, including a professional senior-management team.

This information highlights repeat business from the established customer base and relationships with municipal councils, which it associates with year-on-year loan portfolio growth.

7. Key Activities prioritized for recovery:

- Essential Financial Processing: Maintaining key operational workflows, including customer payment processing, loan disbursements, and collection activities.
- Data Protection & Privacy: Safeguarding customer personal and financial data to ensure integrity and confidentiality.
- Regulatory Reporting: Ensuring capacity to provide data for submitting statutory returns and required regulatory filings within mandatory deadlines.

8. Action Plans for Recovery

Critical Financial Services (Disbursements & Collections)

- Backup Payment Gateways: Automatically switch to a secondary bank or payment gateway if the primary system fails.
- Offline EMI Receipts: Submission of Cheques/ Deposit slips to Loan Officers (LO) for collections if internet connectivity drops or cheque bounces, syncing records once back online.

Customer Personal Data Protection

- Restore from Encrypted Backups: Recover customer accounts and transaction ledgers from secured cloud or off-site backups.
- Access Reset: Reset user passwords and enforce multi-factor authentication (MFA) across all staff before logging back into data systems in case of many mishaps.

Regulatory Reporting

- Manual Data Extraction: Pull required financial data directly from verified backup database if automated reporting tools fail.
- Notify Authorities: Inform the regulator or bank partners promptly if a system outage threatens to delay mandatory filings.

9. Information Security and Cybersecurity:

DCCL ensures robust information security and cybersecurity measures, including:

- Implementing a maker-checker system to prevent errors or misuse.
- Safeguarding sensitive information through end-to-end encryption for mobile financial services.
- Using digital signatures for authentication of electronic documents and fund transfers.
- Establishing data access controls to restrict unauthorized access to critical information systems.

10. Data Back-Up and Restoration:

Company's software database is backed up daily using Amazon Web Services (AWS), a widely adopted cloud computing platform. These backups support data protection and enable recovery in the event of data loss, system failure, or other disruptive incidents.

In the event of a disruption: Clear communication channels will be established to notify key stakeholders, including customers, employees, and regulatory authorities.

11. Three-Year Growth Strategy

This report describes the following assumptions and planned initiatives for the Company's three-year growth plan:

- Expand Micro-LAP, MSME working-capital loans across Rajasthan, West Bengal, Jharkhand and Bihar.
- Add 15 branches in Bihar, Jharkhand and Rajasthan and if feasible in other states including West Bengal, while expanding the reach of existing branches through spoke/sub-branch locations.
- Consider converting spoke/sub-branches into fully operational branches after they achieve the Company's specified business benchmarks.
- Recruit an average of five additional field staff per branch each year.

- Extend business coverage to Tier 3 and Tier 4 cities and rural areas across West Bengal, Rajasthan, Jharkhand and Bihar.
- The promoters intend to infuse additional capital as and when required by business needs.

12. Review and Approval

The Board of Directors plays a critical role in the oversight of the BCP, conducting periodic reviews and approving necessary updates. The Board ensures that DCCL's business continuity strategies remain effective, relevant, and aligned with regulatory requirements.

Further, the BCP shall be reviewed annually by the BOD as mandated by the RBI.