arriba inclusive finance pvt. ltd.

CIN – U65929TG2019PTC129904

ARRIBA INCLUSIVE FINANCE PRIVATE LIMITED

IT POLICY & SECURITY MANUAL

Table of Contents

1. Introduction

Information Technology at Arriba covers hardware and communications infrastructure, software and analytic applications, and information and media assets. This 'IT Policy and Security Manual' provides the broad-level framework along with details of procedures for Arriba's use and management of technology for its business objectives. The document specifically addresses the issue of security across Arriba's technology environment, including how inappropriate access or misuse of assets is prevented, and how sensitive data and physical assets are protected.

1.1 Company and Technology Overview

Arriba Inclusive Finance Private Limited (Arriba) is a member of the informal sDevNet.org group of community development organizations, serviced by technology partner eCubeH Research Labs in its social outreach initiatives. The name eCubeH (e^3H) references the focus on technology solutions in the domains of economic initiatives, education, environment and public health for disadvantaged communities.

With guidance from its technology partner, Arriba has since inception in 2007-08 exclusively used free and open-source software and tools based on Linux. eCubeH supplies technology support to Arriba in the form of real-time web and mobile applications for microfinance, accounting and human resources, as well as guidance on all aspects of information management. Arriba also has access to a hybrid cloud with the private component being an in-house managed cloud services facility, interfacing with its applications on the field, and with external partners. Software solutions are developed by a small coordinated team in an agile manner, applying a continuous delivery process and overall facilitating a proactive approach to servicing a dynamic and demanding operational environment. Being close to operations allows the development process to be exceptionally responsive, and further allows the software to develop in a robust manner with strong and immediate feedback loops. This unique setup enables Arriba with a level of flexibility, security and speed that is relatively uncommon in the sector.

1.2 Purpose of IT and Security Policy

The IT Policies and Security Manual contains detailed guidelines and protocols for usage of various assets at Arriba, covering aspects like access control, asset management, incident management and compliance. These policies are designed to provide protection for its assets from internal and external threats. Adherence and compliance to these policies ensures that the access to resources and sensitive data is safe and secure.

1.3 Policy Scope

This IT Policies and Security Manual applies to all employees, partners and third-party service providers dealing with Arriba whether on company property, connected remotely via any networked connection, or using company equipment in any location. All Arriba users need to ensure implementation and compliance as mandated in this document and ensure all regulatory submissions are done in time.

1.4 Compliance Monitoring

Arriba has an MIS team managed by an MIS Manager, covering the entire gamut of responsibilities related to technology development and use at Arriba – ie, hardware and communications infrastructure, database

management, security, user support and interfacing with external agencies. A separate Technology team is responsible for applications development and guidance covering all implemented technologies including server configurations. The two teams coordinate and function seamlessly as a single unit, and the MIS Manager is the key person overseeing both groups at a management level. The MIS team is thus the owner of all policies and procedures related to technology and information security as documented in this manual. The MIS team ensures compliance of all policies and procedures for audit purposes as well as for all regulatory submissions as required. A member of the MIS team takes on the role of Information Security Manager, reports to the MIS Manager, and oversees implementation of security issues at the organization level.

Arriba users engaged in various operations and company tasks continually exchange technology resources, data and information internally with each other, and externally with various partners and clients. Hence information security, proper handling of IT assets and ensuring security of the business environment is paramount. Any non-conformance or non-compliance can severely impact operations and growth. Arriba takes a proactive approach in identifying threats and taking adequate actions to restrict any negative effects. Non-compliance of any activity is first reported to the MIS department. Subsequent escalations are to be done to the concerned department head and management team if required. Standard escalations hierarchy is followed for issue reporting and resolution.

1.5 Review of IT Policy and Security Manual

An annual review of the IT Policy and Security Manual is conducted to

- Incorporate information regarding applications of new technologies
- Incorporate information about updated internal structures
- Incorporate information about any new regulatory requirements
- Ensure effectiveness of policies and procedures
- Consolidate changes in security measures for better safety of all business processes
- Integrate post-analysis recommendations from any security incident
- Assess cost and impact of controls on business performance
- Incorporate any changes in the IT infrastructure and software systems
- Comply with client requirements or guidelines

2. Technology and Tools at Arriba

2.1 Values and Principles

Arriba's technology applications are built over the Common Appropriate Technology Platform (CATP) devised by eCubeH for seamless information sharing across multiple social sector domains. Core principles of the philosophy include (for more information see http://sdevnet.org/content/welcome-ecubeh-research-labs):

- Exclusive use of free, open-source platforms and tools
- Emphasis on a distributed, collaborative effort with control residing at area of operations
- Emphasis on breaking the Digital Divide, with engaged participation from communities being served
- Emphasis on network building, sharing and support services
- Giving back to the FOSS Community

2.2 Technologies in use at Arriba:

A key element of Arriba's technology approach has been to exclusively use free and open software (FOSS). Since inception in 2007, Arriba has not spent any money on any commercial software, barring rare exceptions when necessary to accommodate external partners or regulatory agencies. This has been possible through continuous research and customization of existing FOSS offerings, as well as development of in-house solutions for domain applications. Arriba's web services and mobile applications are all built using standard open-source development tools. A similar philosophy is applied for cloud services, both the on-site facility and the public cloud.

2.2.1 Enterprise Web and Mobile applications:

The Microfinance Streams suite of applications is built over the eCubeH Common Appropriate Technology Platform, using standards-based web and mobile technologies over a LAMP stack. These end-to-end enterprise solutions are built for use on tablets/mobiles, netbooks, desktops and servers. The web applications are accessible via browsers, while the mobile applications are built for Android phones and tablets. They currently include the following:

Portfolio Streams: Currently at version 24.0, this web application includes full-featured microfinance functionality covering:

- MicroCredit | MicroSavings | MicroInsurance | MicroPensions
- Microcredit methodologies: JLG | SHG | Individual
- Nightly Automated Institutional Consolidation
- Role & Designation-based access controls for users
- Client privacy controls
- Online transactions (NEFT, UPI etc.) with SMS acknowledgements
- Flexible product definitions (interest calc methods, frequencies, etc.) facilitating quick product introduction
- Banking Correspondent support
- Real-time Credit Bureau inquiries

- Daily Deduping Checks
- Detailed tracking of loan appraisal process, with Credit History
- Elaborate cash controls at each level
- Automated voucher creation, linkages to GL Accounting System
- Daily aggregated statistics across every level
- Huge library of Reports
- Utilities for microfinance:
    - Meeting day changes; Staff substitution; LUCs; Write-offs;
    - Operational restructuring (branch/center mergers, member dropouts/rejoin, etc.);
    - Moratorium; NEFT reversal; Portfolio buyouts, etc.
- Integrated Social Performance Management

Portfolio Streams Mobile: Implemented since 2014 and currently at version 13.0, this software for tablets & phones provides portfolio information on demand to staff while on the field, and allows transaction updates and related functions. Staff can review member and microfinance product details, and conduct all their transactions in real time. When connectivity fails, transactions can continue to be recorded locally with server synchronizations and related support features (SMS acknowledgments, etc.) occurring once network connectivity returns. Features exist for recording enrollment of new members, social performance management, credit bureau checks, applications and approvals for loans, SMS acknowledgments for collections, support for non-credit micro finance products, etc. Senior staff can conduct higher level activities such as loan approvals, voucher confirmations, branch cashbook closing entries, etc.

Loan Appraisals: Currently at version 4.0 and available in web and mobile modes, this application supplements the Portfolio Streams loan appraisal process. It integrates with the portfolio software for household, member and loan information and credit history, and adds detailed purpose-specific appraisal detail for 27 loan purposes, together with a photo library of loan utilization records. The information tracked will be part of a data-pipeline into an upcoming ML risk-modeling function.

Bean Counter: Currently at version 3.0, this is a General Ledger accounting system. At the core is a multi-level Chart of Accounts that is managed and periodically upgraded in a flexible manner. Hierarchical levels of operational units can be set up, with accounts tracked at each level as well as with consolidation across levels. Multiple types of double-entry accounting transactions are allowed through an easy-to-use voucher entry interface. A rich library of reports including standard financial statements and ledger reports etc., can be generated for any time period, for any operational unit or aggregated unit at multiple levels of hierarchy. Portfolio transactions are automatically configured as vouchers from the portfolio software and transferred / integrated into this system.

People Power: Currently at version 2.0, this is a Human Resources module. At a base level, complete staff level background details are recorded. It is primarily built for payroll functionality within the Operations teams. The software offers features for recording components of salary, attendance, staff leave, staff loans, advances and payroll deductions, together with the final payroll slip.

2.2.2 Cloud Services:

Arriba has access to a hybrid cloud for serving its applications and other systems requirements. With an emphasis on real-time services, Arriba has worked with eCubeH to develop an in-house cloud services facility, allowing for a high degree of configuration and flexibility in scaling up. An array of 30+ commodity servers are housed in the facility, all assembled and configured in-house and running exclusively open-source systems and services together with eCubeH/Arriba applications. This facility is termed EDC, ie eCubeH Data Center. The primary OS in use is the Rocky Linux distribution, a downstream, binary-compatible release of RHEL, ie Red Hat Enterprise Linux. Historically the CentOS community OS was used as the server OS, but with IBM's acquisition of Red Hat in 2018-19, followed by changes in the CentOS structure in 2020-21, global subscribers have mostly migrated to other downstream releases of RHEL of which Rocky Linux is considered the primary successor, being managed by one of the original founders of CentOS.

The EDC network is secure, with multiple embedded levels of encryption and security. Linux Docker container technologies (now switched to podman) were applied since 2016 to improve server capacity and efficiency by a factor of 20+. The facility hosts web applications, mobile web services, transaction and analytic databases, web portal(s), cloud storage with SFTP services, source code management technologies, etc. The facility is supported by necessary support infrastructure such as temperature control (air-conditioning) and automated power backup switching.

In 2022, the network was expanded to integrate with a parallel network on AWS ie Amazon Web Services, the public component of the hybrid network. A set of servers similar to those on the EDC are maintained on AWS, with server loads periodically being exchanged or switched between EDC and AWS. AWS images that are derived from RHEL & Fedora are used as the OS on these servers. Beyond this, all core tools, applications and the entire containerized environment is the same as in EDC. This hybrid facility enables scaling of infrastructure on demand. It also serves as an easy-switch backup in the event of some contingency hitting the primary cloud facility.

Processes are in place for regular switching of loads across the public and private components of the hybrid network.

3. Information Security Organization

Information security at Arriba is organized and managed upon industry best practices. Various security guidelines ensure that the security policies remain in synchronization with the business, its concerns and the operating environment.

Arriba deals with critical and business sensitive information of its clients in addition to its own confidential data. There are also multiple types of financial transactions that need adequate authorization through stringent secured systems only. All data is stored in protected storage solutions, with access staying restricted to identified departments and users only.

3.1 Team Design Principles

Key principles considered in building the information security organization are:

3.1.1 Information Security

Arriba ensures that competent resources are available to adequately support and ensure compliance with all regulatory requirements as listed by RBI or any other governing body from time to time. While a specific (MIS) department is tasked with ensuring the upkeep of all the assets and securing them from threats (physical and cyber security), the onus is on all users to ensure security and maintenance of the assets allocated to them. Strict control is kept over financial transactions, system workflows and data integrity. It is mandatory for all employees to undergo Security awareness trainings at least once every year. These programs are conducted quarterly to train staff on maintaining security protocols and handling critical client data. It is compulsory for every new hire to undergo this training before they join Arriba. Also, all new hires, consultants or any third-party service providers managing critical functions or handling client data are required to sign a scope of work contract which contains confidentiality and non-disclosure clauses. Arriba reserves the right to reprimand in writing, suspend, discharge, or take other appropriate disciplinary or corrective action against any party for non-compliance with information security policies.

3.1.2 Segregation of duties

For maintaining data trail and detection in case of frauds and unauthorized access, it is important to have clear segregation of duties. Also, the initiation of an event should be separated from its authorization. User roles and team structures are defined at Arriba so that there are no overlapping duties. There is clear segregation of duties to ensure that no single person has complete control over the information system environment. While designing the scope of work for team members it is ensured that to access a critical function authorization for two or more members is mandatory. Critical business and technology teams are organized such that there is always one person checking over another. The role-based access and responsibility matrix is used in assigning tasks to teams such that individuals are not assigned to two teams which may have a conflict of interest. The following duties are independently managed:

- Applications Development
- User Support Services
- Cloud & Systems Services Management

- Database and Information Management
- Security Management and Security Audit

The design and access control mechanisms are in place to ensure integrity and security where segregation is not feasible. It is recognized that processes appropriate for small, quick-moving teams and organizations are not the same that are necessary to apply at large organizations.

3.1.3 Maker-Checker

Sensitive company data is always at the risk of phishers and hackers. In the presence of dual approval, systems can catch and block the activity of this kind. Maker-Checker is one of the most important principles of authorization in the information systems of financial institutions. Arriba implements this principle in all essential processes and systems. All financial transactions and expense approvals have dual approval or dual authorization requirement. In all such critical scenarios, the maker, generates or creates the request for approval and the checker, is responsible for checking, verifying, and approving (or denying) the request. This also reduces any errors that might have been missed by the 'maker'. The same principle is also implemented in the portfolio software where vouchers, loan appraisals, cash payments and other critical transactions recorded by field staff are checked and authorized by a senior member and/or MIS team member. Other HR, accounting software and technology tools also utilize this principle extensively where pre-authorization and approvals are required for all critical functions and data entries.

3.2 Information Security Organization Structure

Key components of IT and Security Organization ensure policy making, implementation and revision of policy and procedures as per the changing business environment and technology needs.

3.2.1 Information Security Team

The Information Security Team (IST) is comprised of the MIS Manager and the Information Security Manager (ISM), with oversight by the CEO. This team assesses and coordinates the implementation of information security controls. The IST is the owner of IT Policy and Security Manual and reviews and updates this manual on yearly basis.

The IST meets at least once every quarter to

- Review action items from previous quarter report
- Identify changes in external and internal issues that are relevant to the information security management system
- Review all security incidents and formulate the corrective actions
- Evaluate results of risk assessments
- Identify risk mitigation strategies
- Provide feedback on security performance, monitoring or measurement results, and review non-conformity on audit reports
- Identify opportunities of continual improvement and changes to information security management system

Arriba maintains records of all IST meetings. The IST is expected to maintain appropriate contact as necessary with law enforcement authorities or other government departments, and also with information service providers and telecommunication operators to take proper advice in the event of any significant security incident. The IST may connect with security groups and industry forums to exchange information on latest security developments. The IST may also seek specific information security advice from external consultants when required.

3.2.2 Information Security Manager

The Information Security Manager (ISM) serves as the focal point for addressing all information security issues, and is also responsible for driving policy creation and building security awareness across the organization. This role is responsible for preparing, maintaining and communicating IT Security Policies and Procedures throughout the organization. As a member of the MIS team, the specific individual taking on the role is appointed by rotation across senior members of the MIS team. The security role covers security issues across hardware and communications infrastructure, software applications, and databases. The ISM

- Enforces implementation of IT Security Policy and Procedures relating to application systems.
- Enforces logical security measures for applications and support systems such as servers, databases, Operating Systems, etc.
- Maintains full compliance of the IT Security Policies and Procedures.
- Organizes quarterly information security awareness programs and pre-joining training programs.
- Ensures that the physical security staff is adequately trained to meet security requirements
- Manages the timely resolution of all security issues, and answers any questions regarding IT security management at Arriba
- Ensures that responsibilities are defined and that procedures are in effect to promptly detect, investigate, report and resolve IT security incidents
- Supports the risk management process by analyzing threats to the computing environment
- Monitors all security reports and coordinates with the IST to initiate protective and corrective measures if a security problem is discovered
- Recommends any new security products or security procedure to be implemented for monitoring and reacting to system security warning messages and reports
- Seeks legal guidance and supports legal proceedings in case of illegal data loss or hacking
- In co-ordination with Internal Audit Team, incorporates appropriate procedures in the routine audit checks to verify the compliance to the IT Policy and Security Procedures

3.2.3 MIS Manager

The MIS Manager at Arriba has a broad role covering all aspects of technology management, including hardware and communications infrastructure, software and analytic applications, data, information and media assets, user support, interfacing with external agencies, and importantly, maintenance of security across the environment. The Information Security Manager reports to the MIS Manager. In the hardware and infrastructure responsibility of the MIS Manager are included IT assets such as servers, networking and user device assets. While the ISM primarily focuses on application and information security, other members

of the MIS handling hardware and infrastructure focus on security related to these. In overseeing this activity, the MIS Manager

- Ensures that all infrastructure and data resources are protected from unauthorized access
- Initiates corrective measures on security breaches, and reports all such cases
- Enforces logical and physical security measures over communications systems (e.g., leased lines, routers, switches, WAN, Internet, E-Mail, etc.)
- Assesses vulnerabilities in the available communications system, monitors Firewall and Router Security, and reviews network logs and WAN incidents
- Responsible for maintaining the integrity and confidentiality of data traveling over the network.
- Coordinates with all third-parties to ensure for minimum downtime of communication infrastructure.
- Reviews LAN security parameter settings and ensures that user privileges at the LAN level are based on a "need to know / need to do" basis.
- Monitors network security breaches, unusual login times, password change history, locked-out user-ids, etc.
- Reviews to ensure that physical and logical security procedures related to user device security (ie, for desktop/laptop, mobiles, etc) are being followed (e.g., procedures to maintain inventory of computer equipment, use of screen saver and boot-up passwords, etc.).

3.2.4 Internal Audit Team

The Internal Audit Team carries out internal security audits and maintains these records. Internal audits are conducted annually and are intended to cover all areas of technology and information security. The internal audit team holds responsibilities to:

- Design, implement and maintain the audit, including the frequency, methods, responsibilities, resource requirements and reporting, taking into consideration the importance of the processes concerned and the results of previous audits.
- Define the timelines, criteria and scope for each audit.
- Ensure that the results of the audits are reported to relevant management teams.
- Document information, evidence and result of the audit.
- Presents reports on followup compliance to management teams.

In certain cases, Arriba employs external consultants for conducting the audits to ensure objectivity and independence.

4. Asset Management Policy

Arriba follows an Asset Management Policy to protect business assets and interests. It ensures that assets are properly allocated to end-users to optimize usage and workplace productivity. Asset management practices are used to simplify technical support and maintenance requirements. The goal of this policy is to protect the confidentiality, integrity and availability of Information Assets and Information Systems. The three main objectives of this policy are to ensure an appropriate level of protection, proper classification and well-defined ownership of the information assets. The scope of this policy covers all information and technology assets owned or leased by Arriba, its employees or any third party. The Asset Management Policy is reviewed annually by the ISM and the IT team members.

4.1 Inventory of Assets

Arriba maintains the following mechanisms to classify and protect sensitive IT Assets:

- All information assets are recorded on the Inventory Master Register. All details of the computer equipment and information assets are maintained, including:
    - Software assets (including application software, system software, dev tools/utilities)
    - Physical assets (including computer & communications equipment, media, specialized technical equipment)
- All assets are labeled as per the value and sensitivity
- User and Role based controls are used for data viewing, inserts and updates
- Encryption is used for sensitive data, primarily information relating to KYC, phone contacts, and bank account details

The Inventory Master Register is audited every quarter by the IT team to ensure that all new items procured are entered by actual verification against purchase orders and invoices. The inventory list is cross-checked through physical verification of all assets and proof of such physical verification checks is maintained.

4.2 Asset Classification

All the information assets are labeled as per the classification taxonomy, as listed below in terms of value and sensitivity:

(a) Highly Critical/Sensitive:

- Physical: Server/Network passwords + keys, Backup power
- Customer KYC, Contact and Bank information

(b) Confidential:

- Customer general information including socio-economic and credit records

(c) General:

- Computer Hardware, Temperature Control (AC)

4.3 Asset Ownership

All the identified IT and Security assets have nominated owners. The owner of the asset shall ensure that the asset and the information related to the asset is up to date. The asset owner shall be responsible for defining and periodically reviewing access restrictions and classifications with the IT department to confirm that all access control policies are adhered to. All asset owners shall adhere to all the rules governing the right usage.

4.4 Asset Usage Policy

All users including employees, contractors, consultants and third-party service providers accessing and using Arriba resources shall adhere to the below guidelines on the acceptable use of information, electronic devices and network resources in accordance with Arriba IT and Security Policy.

4.4.1 Usage Guidelines

All proprietary information stored on electronic and computing devices whether owned or leased by Arriba, its employees or any third party remains the sole property of Arriba. It shall be ensured through legal or technical means that proprietary information is protected in accordance with this policy.

- All employees, contractors or consultants or any third-party service providers shall promptly report the theft, loss or unauthorized access of proprietary information to the Arriba IST.
- The access, use or sharing of proprietary information shall be carried out only after proper authorization as necessary. Providing access to another individual, either deliberately or through failure to secure its access, shall be strictly prohibited.
- Arriba reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy. For network security and maintenance purposes, authorized individuals from Arriba may monitor equipment, systems and network traffic at any time.

All Arriba users shall adhere to the IT and Security policies at all times. All below mentioned activities shall be reported to IST

- Usage of Arriba resources for any restricted, unauthorized or illegal activities under local, state, national or international law is strictly prohibited.
- Any violation of copyright, trade secret, patent or other intellectual property, or similar laws or regulations, or the rights of any person or company is unacceptable.
- Installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the user or Arriba is not permitted.
- Unauthorized copying, digitization and distribution of copyrighted material including, but not limited to, files, documents, photographs, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Arriba or the end user does not have an active license is not permitted.
- Unauthorized access to data or assets or any other form of security breaches like disruptions of network communication, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes or accessing Arriba data, servers or accounts for any purpose other than conducting Arriba’s business is prohibited.

- Introduction of malicious programs (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) into Arriba's networks or servers, revealing specific users account passwords to others or allowing use of an account by any other person or entity, is forbidden.

4.4.2 Highly Critical or Sensitive

All documents, removable media or files containing "highly critical or sensitive information" are marked "Critical" along with the Arriba name and logo. The IST team shall maintain a list of all such assets, with details of the name of originator, date of development of document, version clearly defining the access control for authorized users. The replication or exchange of information from these restricted assets is permitted only on prior authorization from the owner and should carry suitable legends like "Critical" for better control. All restricted information if shared over an open network should be protected by encryption. If the restricted information is sent in hard copy through post mail, then it must be sent in a sealed envelope and must have mark-up in bold "To be opened by Addressee only". All documents or removable media containing "highly critical or sensitive information" is stored in a locked enclosure when not in use. All of the above applies specifically in the case of unencrypted assets in order to secure them.

4.4.3 Confidential

All documents, removable media or files with readable confidential information are put in separate folders and marked "Confidential" along with the Arriba name and logo. Such assets are recorded by the IST with details like name of originator, date of development of document, version and clearly defining the access for the authorized users. Any replication or exchange of such assets is to be carried out only by the authorized users or with prior permission of the owner, clearly disclosing the access and disclosure responsibilities to the receivers. All documents and removable media containing "confidential information" shall be stored in a locked enclosure when not in use. For electronic transmission of confidential information, emails should be clearly marked as "confidential". Also, for such emails preferably a secure email system is to be used and emails are to be encrypted as required. For sharing confidential information through regular post, a sealed envelope with "Confidential" marking along with Arriba name and logo is to be used.

4.4.4 General

All general and non-critical assets do not require any labeling or marking. For these assets no restrictions are imposed but precautions must be taken to check any misuse.

All users shall comply with the above policies and procedures for data and information security.

4.5 Transfer or Return of the Asset

In the event of role change or termination, the MIS team ensures that all assets in the ownership of the user (ie, employee, partner or client of Arriba) are returned. This process is initiated and authorized by HR and the supervisor. The assets owned by the user can be any hardware, software, data or any policy or procedure manuals or technical documentation or it can be any keys, passes and other access devices. In case of termination the MIS team will deactivate access to various Arriba resources, delete individual access identifiers and remove access authority granted to such users.

In the event of transfers, the access rights and ownership are modified as required for the new role. On completion of the transfer or return of the assets, the IT team shall notify the HR Department of the completion of the transfer or return with the list of assets.

5. Access Control Policy

Access control at Arriba is implemented through physical security measures and through appropriate system settings for logical access to network, computing resources, applications and utilities, and data as per the privileges specified for each user. The objective of this policy is to limit access to information and systems based on need. This policy is designed to maximize the level of security and minimize the risk of security breaches by tightly controlling who, when and how can access different technology systems and information at Arriba. There is a formal process for user access provisioning for various systems and services. Every quarter the ISM together with the MIS Manager review the access privileges for all users. A detailed log is maintained to record user id and time stamp for every access to networks, applications, databases, devices and premises. These logs are also monitored by the MIS team and reviewed by the ISM once every quarter. The IST reviews and updates the Access Control Policy annually.

5.1 User Access Management

At Arriba, there is a formal process for user access management

1. User registration is initiated by a communication from the HR or the Operations team. As per the registration request and the user role requirements, the MIS team creates the email id and defines the role-based access for the user to the applications, network and other services. All activities related to user creation, user deletion, or change in profile are raised to the MIS team via email request. All such requests are either initiated by the user on approval from the supervisor or by the supervisor or the HR team.
2. Change in user access can be initiated in the following scenarios:
    a. Staff Exit: The supervisor starts the handover process for the leaving employee and reassigns the roles and responsibilities as required. The exit process with MIS is initiated by an email communication from HR or the supervisor. The MIS team carries out the task of removing the access rights, suspending the user ids and email id as required. MIS checks that all access privileges associated with the employee like VPN, remote access, cloud services, shared drive or any other services are revoked. An email auto forwarding is set-up for the inactive account if necessary. MIS informs the HR and the supervisor after completing all exit formalities. All other procedures like handing over the media, keys or any other assets and other exit formalities are also carried out before the last employee's day. All admin staff and security managing entry to the office premise are made aware of the employee exit. To receive the exit clearance the employee completes the handover process and receives a No-Objection sign-off from various departments like MIS, admin, security, HR and others as per the role.
    b. Staff Transfers or Change in the Role: Center Transfers are managed by the Operations team in coordination with HR. HR or the Supervisor initiates the request to MIS for the user access changes in the case of staff transfers or the change in the role by sending an email communication. The access privileges are modified as per the new role. A new user id is created if required and also other assets are shared with the user as per the new role. The MIS team informs HR and the Supervisor after completion of this change. HR informs the office security, the admin staff and all other concerned teams of the role change. The

Supervisor informs other members of the operations team of this role change or transfer and assigns duties and responsibilities as per the changed role to the user.

3. Area and Office Management Changes: The process of Area and Office Management Changes is initiated by a communication from Senior Management or as a request from the Department Head. The MIS team changes the access privileges and reassigns the roles as required. New user ids or access privileges may be created as required. The ISM reviews all the changes carried out by the MIS team.
4. The logs of user login and activity history on various applications, databases, computer systems and other services are stored in the system. These logs are regularly monitored by the MIS team and can be extracted and reviewed by the department heads or senior management if required. The ISM reviews the access logs along with the MIS Manager at least once every six months and updates and redefines user roles and privileges if required.
5. A user is automatically signed out if inactive and the session expires. The user is then required to log back in. This rule is implemented for all web applications.
6. All privileged account ids are separately managed. The MIS Manager controls access to this data and the ISM reviews it during the quarterly reviews.

5.2 Access Control Rules

MIS at Arriba applies the principle of "least privilege" and "need to know basis" to design the access permissions to the absolute minimum required to function effectively in the specified role. It is ensured that there is consistency between the access control and information classification policies of different systems and networks. User access profiles and rights are designed to manage access in the distributed network environment which recognizes all types of connections.

5.2.1 Network Access

1. By application system design, field users are limited in network access to strictly the branch that they work in and the specific clients that they support.
2. Network SFTP design limits users to a sandboxed chroot environment, where users have access only to their own storage areas and cannot apply any system penetration techniques to escape outside this control area.
3. There is a single privileged account, i.e., the MIS Manager.
4. Logout / Lockout controls exist as below:
    - Currently logs out of web applications after configured session duration limit
    - Clears out all data available to the mobile app if no download/upload within configured limit hours; System requires re-downloads
    - Suspends user of the mobile app if no download/upload within the configured limit days

    Changes planned for FY2022-23:
    - Users are prompted to change the passwords in six months
    - Users are locked out after 3 unsuccessful log-in attempts. The IT team is to be contacted for the unlocking of the account.

5. Access rights for consultants and other third parties are granted only on approval and are reviewed by the MIS Manager on quarterly basis.
6. User access and rights are reviewed by MIS and the ISM every six months. These are updated whenever there is a major change in the assignment of user/s.
7. The authorization of special privileges like the access to third party tools, remote logins, and accesses from networks outside Arriba network are separately maintained and reviewed once in three months by the MIS Manager and the ISM.

5.2.2 Internet Access Policy

This policy outlines the usage of Internet resources, including the use of browsers, electronic mail and instant messaging, file uploads and downloads, and voice communications.

- Users at Arriba are encouraged to use the Internet to carry out responsibilities associated with their roles and further the objectives of the organization. Arriba allows limited personal use of the internet for communication with the family and friends, for independent learning, and for public service.
- Users are required to comply with all statutory & regulatory laws (including but not limited to the Indian IT Act), Arriba policies, and contractual obligations.
- Arriba's Internet and other resources should not be used for illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting personal loans and financial services from external entities, soliciting for illegal pyramid schemes, and computer tampering (e.g., spreading computer viruses).
- Use of the Internet in a manner that is not consistent with the mission of Arriba, misrepresents Arriba values, or violates any rules is prohibited.
- The use of Arriba's resources and internet for mass unsolicited mailings, uploading and downloading of files for personal use, access to pornographic sites, gaming, watching movies, competitive commercial activity and the dissemination of chain letters is strictly prohibited.
- The access for non-employees to resources or network facilities of Arriba unless pre-approved by Arriba management, is not permitted.
- Users shall not view, copy, alter, or destroy data, software, documentation, or data communications belonging to Arriba or any individual without authorized permission.
- In the interest of maintaining network performance, users shall refrain from transfer of any unreasonably large electronic mail attachments or video files not needed for business purposes.

5.2.3 General Controls

- Access to all the computing resources is controlled using User-IDs and passwords for identification and authentication. All the other devices like routers, Wi-Fi servers, etc., also require user ids and passwords for access.

- All the systems are configured with screen savers to lock the system screen after a short period of no use, requiring passwords to access when locked.
- Arriba follows clear desk and clear screen policy to ensure security and safety of assets and information.

5.2.4 Password Rules

- All Passwords are to be kept secret and confidential by the individual they belong to.
- The passwords are exclusive to the user, unless explicitly specified by the IT team.
- Strong and unique Passwords are required for all the users. Passwords require 8 or more characters, with at least 1 from each group:
    - [a-z]
    - [A-Z]
    - [0-9]
    - special characters: [!@#%&-_]
- All users are advised to change the passwords for email access as well as for the applications on an annual basis to contain any unauthorized access.
- Secure password distribution mechanism is used
    - Passwords shall not be shared in full in plain text,
    - Password shall be transferred in multi-part form
    - Passwords are transferred digitally only in encrypted form
    - Salt/Spice with hashing is used for password storage
- In the case of new email accounts, the user changes the password after the first login.
- Other password related system changes planned in FY 2022-2023 are
    - Users are prompted to change the passwords in six months
    - Users are locked out after 3 unsuccessful log-in attempts. The IT team is to be contacted for the unlocking of the account.

6. Operations Management

Operations Management covers all IT infrastructure, including the applications, services, hardware, networking, and communications. The goal under this framework is to monitor and control IT services and infrastructure, as well as enable normal operations required to keep applications, services, and hardware components running in a stable manner, staying available when needed. The availability, efficiency, and performance of an organization's processes and services are all ensured by effective IT operations management. The operations management at Arriba is planned and designed to ensure consistency, stability, and quality in IT services, deployment, and support.

6.1 Operating Procedures

All operating procedures are documented via formal processes, and changes are submitted to management for authorization. These procedures specify the detailed execution of each job including:

- Processing and handling of information
- Instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions that may be applied in such cases
- Contacts for support personnel in the event of unexpected operational or technical difficulties

A set of specific operating tasks and events are listed below together with associated procedures.

6.1.1 Server restart and recovery

In the event of a system crash, the recovery procedure is documented and visibly available in the server room, by the present infrastructure and equipment. It is reviewed and updated periodically with any change in the technology environment or upgrading of equipment. Steps for system recovery are

1. Check the server operating system. If necessary, reinstall (Fedora/CentOS/RockyLinux) from the saved image.
2. Often it may be more appropriate to install the Unit Server using the saved US clone image.
3. Configure eCubeH applications as necessary, (ie, for Portfolio Streams, Bean Counter). Ensure application access to necessary databases.
4. Configure Server IPs, ports etc.
5. Test the server from internal and external networks.
6. Configure user desktops or share updated URLs to use eCubeH applications.

6.1.2 New Purchases

All new purchases are done in accordance with the IT Policy and Security manual and other organizational policies. The MIS team identifies the requirements and standards for various technology equipment to be used by Arriba in line with changing market and technology trends. All requests for purchases take into account the longer-term organizational business needs. Purchase of new computer and peripherals requires careful consideration since it involves significant expenditures, and is expected to be used over a multi-year period. Vendors and suppliers with a proven service record are used for new purchases, while pricing is verified across online channels and multiple distributors of the items. All computers and technology

equipment are fully and comprehensively tested and formally accepted by the MIS team and the ISM before being transferred to the live environment or user sites.

6.1.3 E-waste Disposal

Arriba has a robust electronic waste management policy. Through this policy, Arriba reaffirms a commitment to environmental protection by ensuring proper E-waste management. It is the endeavor of every user at Arriba to maximize utilization of all IT assets to their full productive life. Apart from internal re-use, options are explored to extend use outside through re-using the parts in our partner networks. Only such IT assets which are non-operational and cannot be reused for any other alternate purpose are considered as IT E-waste for disposal. The MIS Manager takes the decision on this. All Arriba project offices dispose such E-waste through an empaneled vendor, who is registered with the State Pollution Control Board as a certified dismantler/recycler. Further, all the new technology products are procured from the vendors who have the capability to collect, buyback and dispose the product in eco-friendly manner.

Arriba users are required to take the necessary steps to purge confidential data residing in the hardware and also keep a back-up, to the extent deemed essential, before disposal of the E-waste. The users are trained on this during the IS awareness training programs. Besides, a proper record of all E-waste handed over to the vendor would be kept on record for possible scrutiny by delegated State authorities. The MIS team coordinates the implementation of this policy across all Arriba locations.

6.2 Change Management

Formal change management procedures are documented and enforced at Arriba in order to protect information systems from vulnerability or corruption. All change management including any new feature additions or application development follows extensive multi-level testing, piloting prior to rollout, and also continuous monitoring through the production phase. This approach has served well through a vast number of releases of various web and mobile applications, and no known security incidents have been recorded. Software, systems and applications are all developed internally in the Linux environment, primarily RHEL derivatives known for high security. Applications are developed in-house over the Linux operating system using the eCubeH Common Appropriate Technology Platform.

The scope of change requested is reviewed by the Information Security Manager and the MIS Manager to ascertain the impacts on the existing security systems as well as on the partner's environment. The development, testing and production environments are separately managed by the MIS team. The changes requested are first implemented and tested in the Test Environment and are later transferred to the Production Environment after completion of all necessary internal processes.

The Change Management Process is as follows:

6.2.1 Definition and Documentation

All the user or client requested changes are clearly defined after an iterative process of requirements gathering. The functional and non-functional requirements that the system has to deliver are captured. In

the event of updates to existing functionality, all the gaps in the current system with respect to the desired functionality are evaluated. The data impacted from this change is collected and analyzed. The scope of the change is documented once it is approved by management.

6.2.2 System Design and Development

Performance, modifiability, availability, scalability, reliability, etc. are important quality requirements in the system design. While designing the new system, the scale of the system, network bandwidth usage and other performance parameters are analyzed.

6.2.3 Preparation for change

Top management's commitment towards any change initiative is crucial. Senior management of Arriba plays a vital role in defining the change management procedure by providing clear and consistent directives to the teams involved in the process. The MIS team prepares the organization for this change and makes the necessary modifications in the policies and procedures as required. Repeated and consistent communication throughout the implementation process to remind team members why change is being pursued, is extremely important. The MIS team in coordination with the ISM designs the communication strategy. It ensures there is sustained interest and engagement of users with the new IT implementation. It also creates an in-house training plan for the teams impacted by the change. The MIS team reviews various controls and integrity procedures to ensure that they shall not be compromised by the changes.

6.2.4 Multi-step Testing

Application development is followed by extensive multi-level testing/piloting prior to rollout, and also continuous monitoring throughout the production phase. All hardware changes, software changes, and new releases are tested before being implemented in a production environment. The MIS team performs various manual tests to validate that the change functions as desired. Since the technology teams are very close to operations and the operations teams, there is natural clarity on requirements and development takes place rapidly and in a relevant manner. Users are active in and exposed to the development process as it happens, to give real-time inputs. Thorough testing is conducted against live databases in a sand-boxed test environment. Testing is carried out to check the desired functionality is operating well, desired performance goals are being met, and if any new potential defects are identified. Arriba uses the subversion tool for source code management, and can easily revert back to older releases, but such drastic steps are never needed, due to the proximity to operations. If any further changes to meet the stated functional requirements, fix new bugs, develop additional capabilities for improved functionality or performance, etc are required as determined by testing, the development team works on it in real time and then the testing is repeated.

6.2.5 Implementation

Once the changes are approved, the implementation is carried out in the Production environment ensuring that the implementation of changes takes place smoothly without disturbing the business processes involved. For example, new application releases are often done on weekends during off-periods. Changes are continuously monitored and all incidents are logged. Post-release training sessions especially during new software releases are conducted at user sites as required.

6.3 Software Version Control

Arriba uses the 'subversion' tool for maintaining multiple revisions of team-built software through the development and release process. Arriba users use only in-house built software for all application purposes. Staff members of Arriba are required to undertake all precautions and abide by the organization's policy on software protection, namely

- The operational system shall be updated only after authorization by the MIS Manager / System Administrator.
- The updating shall be as per the instructions of the MIS team / vendor / manufacturer.
- The updating in the production environment shall be done only after successful testing in a test / development environment.
- Previous versions of software shall be retained as a contingency.
- Critical fixes in application software after a release may be issued as an interim release, otherwise application feature updates are usually issued in fixed releases
- Server security patches for Rocky Linux and AWS Linux images are issued on a regular basis. Arriba is exploring a monthly timetable for applying security patches to its server systems, in line with the calendar for system switching between EDC and AWS environments

Arriba employees shall notify the IST promptly of any misuse of software or unauthorized usage of resources which comes to the staff member's notice.

6.4 Capacity Management

Capacity Management ensures that information technology resources are sufficient to meet upcoming business requirements cost-effectively. This includes:

- Processors
- Storage
- Networking
- Communications systems
- Software applications
- Printers
- MIS tools

Capacity Planning is an annual exercise at Arriba, and also when a significant systems change is planned or during emergency situations. These include new system requirements as well as projected trends in computer and network use of current systems. Monitoring and trend analyses of the utilization of key system resources (physical and cloud) are to be performed quarterly.

6.5 Personnel Management

Arriba's MIS team is composed of technical staff with a diverse set of capabilities and backgrounds. Well-defined process of selection, orientation and induction by the HR and MIS team ensures the efficient workforce is available for various tasks. The employees undergo continuous training on essential and new technologies and procedures from time to time. These training programs are also updated and upgraded

every year. Each team ensures that multiple personnel are trained to perform various tasks and there is a back-up available when needed. The team members work closely so that there is always coverage for core tasks like server management, backup, disaster recovery and other critical jobs. In a crisis situation or during work overload, the MIS team members collect transaction information over the phone from the field (manageable since primarily exceptions are recorded), and enter it directly into the applications. Various tools and resources are utilized to increase efficiency and productivity of the workforce. The MIS systems are constantly reviewed and updated through innovations and experimentation to save efforts and time for the employees.

6.6 IS Audit Control

All procedures and policies under MIS and Information security management system at Arriba shall be subject to independent review periodically, as deemed necessary. The review if conducted can be by auditors who are independent of the MIS functions. The auditors can be either external or internal audit teams. If conducted, the following measures for audit controls may be adopted:

- Audit requirements, scope and schedules should be carefully planned to avoid disruptions and to ensure effective coverage.
- The methodology and tools adopted by audit staff shall not compromise security.
- Auditors shall have 'read only' access to data.
- All procedures and work done by the auditors shall be documented.
- Access to information systems audit tools shall be protected to prevent any possible misuse or compromise. Access to such tools shall be available only to the MIS Manager / System Administrator.

Reports indicating vulnerabilities shall be classified as confidential and shall be made available on a need-to-know basis.

6.7 Network Security Management

Any single weakness in one portion of the network can create vulnerabilities that can be exploited to attack or access some other resource elsewhere on the network, hence network security is very important. Network Security Management aims to secure every server, desktop/laptop and all other devices on the network. There are 3 internet lines: (1) Main Line / Network (2) Backup Line / Network (3) Testing Line / Network. Testing environment is separately managed from the production systems and network. The following network controls are in place at Arriba:

1. A comprehensive network architecture diagram for the entire multi-network environment is maintained. The strength of network security derives from a number of approaches: firewall rules, services on non-standard ports, bastion host, OS & application access controls, chroot environments for different users presenting private, sandboxed areas for users, root constraints, encryption of passwords, sensitive data and data transfers, and various other Unix-level controls.
2. Firewall controls and physical access controls permit only the sysAdmin to have firewall access. Company guidelines prevent unauthorized access other than for company purposes. Firewall changes are infrequent, and are documented in detail. Firewall changes are primarily pre-configured port for-

wards for select protocols to server containers. Firewall Controls are managed by the MIS team under the supervision of the MIS Manager. The MIS Manager checks these rules and controls during quarterly Access Review.

3. Database access by web and mobile applications is logged. The log files are saved on servers and are backed up as required. Application Logs are typically stored for a period of 1-2 months on a rotation basis. SysAdmin staff review system and application logs regularly. Any suspicious entry is flagged to the MIS Manager and the ISM.
4. NTP/chronyd are set by default on RHEL derivative systems, enabling a common time synchronization service.
5. Applications use encrypted data and access controls (role-based access and permissions, encrypted sensitive data etc.). Staff access are limited to working with data related to the clients they serve, and further limited by the stage of the client along various processes. Member sensitive data is encrypted (KYC IDs, Bank Account details, Contact phone, etc.).
6. Mobile app users follow two-step authentication as they can login (a) from registered devices (b) using login password.
7. All web and mobile applications use SSL certificates, role-based access and pre-defined user-id with passwords for any end-user transactions.
8. IP Whitelisting, SFTP and other such means for secure data transfer are utilized as per the client guidelines and available infrastructure and services.
9. No use is made of any commercial software, given the more secure, better designed and lower cost Linux-based solutions. There are some rare, unavoidable cases where commercial software is used (e.g., to support banking partners that use the Microsoft platform, or to comply with some regulatory requirement that forces use of such platforms). In such unavoidable cases of commercial software use, only licensed software is used.

Given this highly secure environment, no successful attacks have penetrated into the network in the company's history.

7. Security Measures

Various security measures and protocols are designed and implemented at Arriba to ensure business continuity and information security of its collaborative and distributed work environment.

7.1 Physical and Environmental Security

Server room management

This procedure is designed for the management, safety, and security of the server room. The server room is a restricted area for access and only the users with legitimate responsibilities in the server room are permitted access. Any new user is permitted by authorization from ISM and approval from the senior management on need basis. In case where any third-party users or visitors require an access, they are made aware of this policy and their obligations therein. It is the responsibility of the member of IT accompanying the visitors to ensure they carry out their duties in a professional manner whilst working in the IT Server Room. Additionally, security and cleaning personnel may access for their specific roles under supervision from the IT. Staff seating around the server area is maintained such that the core IT team always has a view of the server room.

Server room has environmental protection equipment installed and maintained for dependable and robust performance. These include fire suppression, air conditioning and power supply. A UPS and battery rack is available to supply power backups for between an 8-to-12-hour period for the servers as well as connected computers within the head office. Also, there is a plan to install CCTV for remote oversight of server room. This is expected to be done in Q1 2022-23.

The use of mobile phones, pagers or other equipment that emits radio waves within the IT Server Room is forbidden unless specific exemption is obtained from the ITM. Food and drink shall not be taken into the Server Room. Movement of all assets in and out of the room is strictly on pre-approval from ISM and Senior management. These movements are tracked and logged by the IT team.

Other Security Provisions

The office premises are in a secure location. All the servers and assets utilized for client operations are secured in a safe area. There is clear demarcation internally of servers used to support any specific bank partner, with such systems protected from access by any unauthorized personnel. Movement of assets is monitored and logged by the IT team. All logs are reviewed by the ISM during the quarterly reviews with the IT team. Night security is provided by resident staff. A night watchman stays by the server, ready to call up the IT team members who reside nearby should there be a crisis. The Access Control Rules are implemented and monitored by the IT team for the office premise and for all the user sites. Physical access rights are also reviewed quarterly by the ISM. Access to critical facilities for any external bank partners or third-party service providers is allowed only on approval from the ISM or senior management.

Environmental conditions are continuously monitored by the IT and manufacturers' guidelines for protecting the equipment are followed by all the users. Mock security checks for various unforeseen scenarios are conducted once a year. Fire drills are conducted semi-annually.
The list of the users permitted in the server room and other critical facilities is managed by the IT team and is quarterly reviewed during Access Rights review by the ISM.

7.2 Equipment Security

Servers are built in-house, configured using an eCubeH process based on the highly secure CentOS distribution of Linux. While Linux in general has very many built-in features for privacy and controlled access (e.g., folder and file permissions, user & group controls), many additional security features have been added by the eCubeH configuration (e.g., CHROOT access on SFTP servers, curtailed access to root user, structured user permissions, use of non-standard ports, selective encryption, etc.). Arriba's servers have never succumbed to external attacks, with users being quite thoroughly shielded.

- Environmental conditions are monitored for conditions which could adversely affect the equipment. Manufacturers' instructions for protecting the equipment are observed at all times. Users are required to protect the equipment from exposure to fire, smoke, liquids, lightning, theft, strong electromagnetic fields, dust, etc.
- Only authorized maintenance personnel can carry out repairs and service equipment. Also, records are kept for all suspected or actual faults and all corrective and preventive maintenance.
- Security controls are applied to equipment sent offsite. Preauthorization is required for removing any office equipment. A gate pass is prepared for taking equipment and software to another site. A record of the movement is to be maintained.
- Suitable precautions are taken by the employees for home working environments such as appropriate lockable cabinets and access controls for computers.
- Whenever a user leaves equipment unattended, it is to be secured with a screen saver with a password and wherever available auto log out/ off settings are to be used.
- Other locking mechanisms available are utilized to protect any resources when unattended or beyond working hours.

7.3 Data Security

Client Privacy is a core consideration in data management at Arriba. Clients have a right to expect that their information is safe, and accessible to a limited set of authorized personnel strictly on a need-to-know basis related to services they are receiving. A diverse and deep set of approaches are followed to ensure the above ranging from technological approaches, management policies on information to be saved, physical security, all the way to personnel background checks on staff interacting with clients and managing their information.

7.3.1 Data Ownership

- The role of information owner shall be determined based upon the following considerations
    - who is the source of data
    - who is responsible for the accuracy and integrity of data
    - who budgets the costs of creating, processing, storing, transmitting and using of data

    - who has the most knowledge of the information asset's business value
    - who would be impacted by a security breach of the information
- The data owner must also ensure that effective monitoring of the controls and protective measures are in place, and that all security breaches are appropriately investigated and resolved.
- The data owners are responsible for assigning appropriate sensitivity classifications (Highly Critical or Sensitive, Confidential or General)
- The data owner defines access authorization to their information and assigns an information custodian if required.
- The data owner specifies and communicates the security requirements to MIS manager, administrators and users.

7.3.2 Data Security Policy

1. At the time of joining, new staff shall undergo induction training conducted by HR which covers topics of client confidentiality and information security.
2. Staff shall indicate acceptance of Company policies by signing on a copy of HR guidelines.
3. After joining, staff shall participate in periodic training programs conducted by IST, especially during the issue of new releases of software. At trainings users are made aware of the critical nature of data they manage and the need to maintain client confidentiality.
4. The client guidelines as per the agreement are followed for data retention, data deletion and secure disposal. Any data as may be required to respond to queries from external GOI authorities (IT Dept, regulators, etc.) in the future is retained. Any external bank partner requirements on data retention are cross checked against meeting the needs of GOI and related authorities and are then implemented as per the agreement.
5. In the event of non-compliance with security policies, the incidents are reported to management and action is taken accordingly. Such incidents may be identified in many ways, such as regular QC checks conducted by MIS. An example would be a case of staff found to have entered loan or KYC information incorrectly. An investigation may be conducted and action taken as appropriate, with the primary focus of ensuring that the incident does not repeat.
6. A structured process is to be followed at the time of staff exit, for removal of access rights and revoking of assets. The process is initiated by a communication from HR or Operations. As per the request, MIS manages both the removal of access rights as well as recovery of assets assigned.

7.3.3 Database Backups

Automated scripts run to produce daily, monthly and annual backups of databases associated with the Portfolio Streams (microfinance) and BeanCounter (accounting) software solutions. These backups are maintained on multiple servers within the eCubeH private cloud facility. They are also maintained on hard drives & DVDs stored at multiple locations – (a) a city-based bank locker, (b) a geographically-distant regional office data center, and (c) personally held with key MIS and Accounts personnel. Finally, the process for automated backing up to a parallel cloud storage facility (Google Drive or AWS) is under development.

Daily:

Cron backup: CATPSystemDB, AggreDB, CoreDB & MobileDB for last 7 days in local server, with a copy to Historical server

Local server: BDC & ADC (ie, Before & After Day-Closing DBs) for the last 60 days

SFTP Server: Branch ADC, roughly 1 month

MIS/Historical servers: Aggre Consolidated/Branch Consolidated for the last 30 days

External HD: Daily BDC & ADC for the last 6 months

Monthly:

eCubeH SFTP server, Historical server & External HD

ADC & Consolidated

Monthly Reports

Annual (post Audit):

2 DVDs created: One DVD kept with Accounts & other kept in the bank locker

DBs (portfolio, beanCounter, peoplePower, CATPSystemDB, Aggre, Core, geoClimatic & Mobile)

S/W (eCubeH folder & all PDF reports (ledgers, etc) for the FY)

Annual Cleanup Files (Historical, Historical_delete, CSV files)

Quarterly Testing and verification of backup

An automated database replication process is carried out across servers on Arriba's multiple networks, so that an automatic switch-over can be triggered in the event of failure of a single system or the entire network. Once every quarter the back-ups are tested to verify data integrity and validate the restoration process. The restored systems, applications and files are checked to ensure that data is valid and accessible as intended. This process is initiated by the MIS team and supervised by the IST. The local backup server and media back-up are tested. It is checked that the critical processes and operations are running as normal.

7.4 Application Security

The application software programs shall be suitably protected from unauthorized access. Arriba's microfinance applications are built on top of the eCubeH Common-Appropriate-Technology-Platform (CATP), allowing for rapid development with data sharing across domains in a secure and integrated manner. Applications have login passwords which are encrypted using powerful hashing technologies. Users have application permissions associated with primary system designation as well as based on roles (i.e., a single user may have multiple roles). These permissions provide or limit access to screens in the application, fields within the screen that are visible or editable, as well as to what extent update features are available.

Access to Mobile software requires prior registration of IMEI numbers and Android DeviceIDs of the specific device, so that only the designated user for the specific mobile/tablet may use the software on that system. Special attention is paid to the '**Sensitive Information**'. This refers to fields such as Bank Account details, KYC IDs, contact information etc., which are deemed to require significantly higher security. These fields are maintained in an encrypted fashion in secondary storage, so that even if someone breaks into a database,

they will not be able to decipher these values. Further, applications do not directly display sensitive data on reports, and even on screens it remains hidden except in the limited set of cases where the context demands it.

Similar to server access, databases have DB users attached with associated access and update permissions. Additionally, there is application-based field-level control, with encryption for sensitive fields (discussed in application security). Daily transaction data in temporary files from web & mobile applications is cleaned up after being posted to permanent files. Arriba's storage servers are based on Secure File Transfer Protocol (SFTP), in which data transfers occur in an encrypted manner. Users have access to limited areas on the servers, based on their file-system permissions. Approaches such as CHROOT, no-access to root users, avoiding use of standard ports, selective encryption of the file system, etc. all add to storage security.

All application modifications are done as per the approved change management procedures and project plan. All major applications may be reviewed for security and internal controls through a system of audit.

7.5 Information Transfer Policy

Arriba users are required to protect exchanged information from interception, copying, modification, mis-routing, and destruction.

1. All business correspondence, including messages, shall be retained as per the data retention policy.
2. Sensitive or critical information shall not be left unattended at public places and users shall ensure that they take appropriate precautions to avoid revealing sensitive information when making a phone call. Special measures to safeguard very sensitive items (such as encryption keys) shall be used as required.
3. All employees shall ensure that they do not have confidential conversations in public places or open offices and meeting places.
4. When exchanging data with other organizations, users shall take necessary precautions such as software copyright, compliance requirements and similar such considerations. Users shall document details as per Arriba policies.
5. In case information is transferred as part of an agreement as per a business requirement, a clear definition of liability and responsibility shall be established by all parties involved. Data exchange agreements shall define management responsibilities for controlling and notifying transmission, dispatch and receipt of data. Minimum standards for packaging and transmission of data shall be predefined and followed during the process. Responsibilities and liabilities in the event of data loss shall be defined and understood by all parties involved.

8. Operations Security Policies

The Operations Security policies are binding for all the employees, consultants and third-party service providers at Arriba. The users are trained on various aspects of security during the Awareness Programs.

8.1 Media Handling

The MIS team at Arriba follows well-defined and time-tested plans and procedures for media storage. It implements security guidelines to ensure the secure management of media to protect sensitive or personal information from intentional or accidental exposure or misuse.

1. Policies and processes regarding use of removable media are communicated to staff, both at the point of initial systems orientation/training, and also at the point of issue of hardware to staff.
2. Regular MIS training sessions especially during new software release also cover policies regarding the use of removable media.
3. Media Hard Disks and Pen drives are always kept in locked drawer/almirah. Transportation of physical media is primarily done by authorized staff in office vehicle for safe-keeping in the bank locker.
4. Unauthorized access, data corruption or misuse during transportation is to be strictly avoided. Only authorized staff is allowed to carry the media in office vehicle, and remains responsible for care of the device against unauthorized access / misuse.

8.2 Work from Home

The MIS team at Arriba ensures information security and supports employees with everything needed to work from home when necessary and appropriate. While working remotely the employees and other users shall follow the IT Policies and Security guidelines.

1. Work-from-home is strictly for managers & HO staff over Google Workspace (mail) and SFTP (i.e., encrypted SSH). Both are secure. About 15 staff fall under this category.
2. Field staff (300+) and MIS team members use web & mobile applications.
3. Applications over web (over SSL, with extensive logging, encrypted transfers, role-based access permissions, etc.) are used by field operations and MIS teams using company-provided & configured Linux systems.
4. Systems are provided to employees with an eCubeH distro (a RHEL derivative, with numerous tools and utilities, and a secure configuration).
5. Mobile apps are used from designated devices only, configured with application software, and supported by extensive logging, encrypted transfers, role-based access permissions, etc.
6. All Sensitive data is encrypted and accessible only for permitted user roles. Users access web and mobile application over standard browsers (Firefox, Chrome, etc.), over SFTP, etc.
7. There is no use of shared desktops / virtualization for desktops, etc.

No anomalous events or incidents were observed for remote users over the company's history.

8.3 Email Usage

1. Requests for creation of new email-ids for new staff is initiated by a communication from HR or Op-

erations. Only the MIS team has the necessary system permissions to create new email accounts.

2. A few email accounts are shared by multiple users. Users are instructed to always identify/record their names on any email submissions. Further, department supervisors regularly review shared email accounts and emails, and users are instructed to not delete any email.
3. Google mail services (G Suite/Google Workspace) are in use. Associated Attachments have a size limit of 25MB, and Gmail virus/spam controls are applied to all mails.
4. Partner bank requirements regarding encryption of data transfers are to be strictly followed. IDBI has a dedicated system configured for data transfers, with automated encryption and transfers to their SFTP server. In the case of IBL, daily transfers of transaction files and other data files (hand-offs) between Arriba and the bank use the IBL's Ganaseva portal.
5. Employees shall use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

All mobile and computing devices that connect to the internal network shall comply with this policy.

8.4 Protection from Malware

With extensive connectivity across networks within the organization and the internet, the proliferation and propagation of viruses is a real cause of concern and needs to be addressed. The MIS team at Arriba has implemented below procedures to safeguard from Malware:

1. Exclusive use is made of the secure Linux environment, together with industry-standard open-source utilities and tools. Web & mobile applications are built in-house over the eCubeH Common Appropriate Technology Platform and standard open-source technologies, with strong standards for security.
2. Arriba exclusively uses robust Linux systems with secure configurations. Since Linux systems when configured properly are fundamentally secure, Anti-virus solutions are typically not required. Anti-virus software is only required on 2 Microsoft systems used to support external partners that are on Microsoft. platforms. These 2 systems are updated with anti-virus software.
3. Firewall rules combined with various other local security mechanisms control malicious code from hitting the network.
4. Frequent reviews of the software and data content of systems supporting critical business processes shall be conducted and the presence of any spurious files or unauthorized amendments shall be formally investigated.
5. All Arriba users shall use only approved and licensed software for all business purposes.

9. Incident Management

An exceptional situation that warrants intervention of senior management is termed an 'incident'. An incident may be the result of unusual circumstances as well as the violations of existing policies and procedures of Arriba. During day-to-day operations. The MIS team may also detect an incident like any hacking attempt or loss or theft of any information, equipment or media, or due to any man-made or natural calamity. All incidents are to be tracked and categorized by Severity and Priority. Various tools are used to extract incident reports and calculate response and resolution timelines.

9.1 Responsibilities and procedures

Procedures are formulated for managing any security breach and for handling incidents. Procedures are established to cover all types of security incidents

1. A quick effective and orderly response to security incidents shall be based on the following escalation matrix:
    a. Initial identification of the security issue may come from the field, and reaches the Information Security Team.
    b. After attempting to resolve the issue, it may be escalated to the technical team.
    c. Senior management may be informed immediately or as appropriate in periodic meetings, depending on the seriousness of the issue.
2. Recurrence of events is to be avoided.
    a. Root cause analysis shall be carried out by the IST and the source of problem be identified
    b. necessary changes in the environment, including hardware, software, connectivity etc., shall be undertaken to avoid a repeat occurrence
    c. Based on availability of new technology and tools, hardening of the internal systems is carried out to remove the possibility of security breach.
    d. Problem resolutions are documented and are used for reference in the event of recurrence. The IST maintains and update the documentation on resolution of incidents and on any system update.

9.2 Response to Incidents

All actions to recover from the security breaches or any system failures are to be carefully and formally controlled by the designated teams.

- Clearly identified and authorized members shall be allowed access to live systems and data. In case of any third-party inclusion, appropriate security controls shall be applied.
- All emergency actions taken shall be documented in detail. Learning from security incidents reports shall be used in user awareness training, as examples of what could happen, how to respond to such incidents, and how to avoid them in future.
- In case any reported incident involves the law, either civil or criminal, the evidence presented shall conform to the rules for evidence laid down in the relevant law. Quality and completeness of the evidence shall be maintained by a strong evidence trail. To achieve admissibility of the evidence,

Arriba shall ensure that its information and security systems comply with a published standard or code of practice for the production of admissible evidence.

- As appropriate and necessary, incidents may be reported to external partners (bank, insurance provider, etc.), by the appropriate teams (MIS, Accounts, Audit and Insurance) on direction from the IST.

10. Business Continuity Management

Backup and Restore procedures in the event of a crisis are documented in the Business Continuity Policy document. System reliability with high availability depends on proper identification and management of key points of failure. Such points of failure may broadly be classified under 3 categories: hardware, services and personnel. Arriba follows an approach of high redundancy to counter the possibility of failure of any single component. The IST ensures that Arriba has sufficient redundant information processing facility to meet the organization's availability requirements in case of any disaster or security incident.

10.1 System Redundancies

Network, system and application architectures are designed for high availability and operational redundancy:

1. Network:
    a. Internally a Multi-Network model is in use. There are 3 internet lines and networks:
        i. Main Line / Network
        ii. Backup Line / Network
        iii. Testing Line / Network.
    b. A primary cloud services facility is maintained in the Bhopal office. Secondary facilities have been explored for setup in alternate regions. While the technical issues are easy to handle, resource constraints for a not-profit and the associated cost-benefit tradeoff have not made maintenance of an alternate facility a practical alternative.
    c. A secondary cloud services facility is maintained over Amazon Web Services. Thus Arriba uses an Integrated Hybrid Cloud (Public + Private), with a parallel setup on a public cloud service. This has been operational since FY2022-23. There is now full flexibility in setup of new servers and services, for scaling as well as for disaster recovery.
2. System:
    a. There is continuous monitoring of systems and servers. No severe issues have been experienced in the past 10 years.
    b. Multiple internet lines and internal power backups are available to deal with contingency issues of internet or power failure
    c. 1-2 Standby Servers are always kept ready & available
3. Application:
    a. Applications are continuously monitored for misuse
    b. Elaborate documented processes are followed through the application release
    c. Continuous testing and field inputs are received through the development phase
    d. Extensive internal testing is conducted through the development phase, and again at the end of the release development
    e. A formal parallel piloting process is followed prior to the stage of release

    No severe issues have been experienced in the past 10 years.
4. Data Redundancy:
    e. Backups are maintained at multiple physical locations currently, and will also be maintained over the cloud, for quick recovery in the event of disaster.

a. Backed up data can be restored in new systems at local site within 1-2 hours.
b. Backed up data can be restored on temporary alternate servers stored at other location within 3-4 hours.
c. With the hybrid cloud option, backed up data will also be set up on the cloud, and servers should be up within 1-2 hours.

The primary problems faced to date are typically (a) ISP downtime and (b) power outages. These are handled with the help of multiple backup internet lines/networks and backup power batteries. Individual components of the existing facility can be replicated in a short period. Fallback servers are available for use in the rare event of any server downtime.

10.2 Business Continuity

Arriba's Business Continuity Plan (BCP) document lists the procedures followed to maintain Business Continuity and manage Disaster Recovery.

10.2.1 Business Continuity Planning

Business Continuity planning exercise to identify and safeguard all critical business processes against any unforeseen adverse scenarios is conducted annually. The critical business processes and the events that can cause interruptions to these business processes shall be identified. The Business Impact Analysis (BIA) to appropriately incorporate the BCP analysis and strategy shall be carried out. The BIA includes the Risk Assessment and Risk Management Processes. All parameters of information security shall be considered while designing the BCP.

10.2.2 Implementing BCP

The primary responsibility for developing a business continuity plan and implementing it lies with the MIS and Security team. The Information Security Team assigns the responsibilities as required in the BCP and provides the necessary support to maintain continuity of service during an adverse situation. It is responsible for the implementation and maintenance of Business Continuity Plan to maintain continuity of service during an adverse situation.

- Copies of business continuity plans shall be appropriately protected in such a manner that the confidential matters are not exposed to unauthorized people and at the same time the plans are available to authorized personnel at times of distress.
- Copies of business continuity plans shall be stored in a secure remote location to escape damage from a disaster at the main site.
- The IST ensures that all the copies of BCP are up-to-date and available when required.

10.2.3 Review and Update BCP

The BCP is reviewed yearly to ensure that all identified flaws and shortcomings are corrected, and new procedures and learning are incorporated in the BCP and the training material as required.

10.3 Backup Management

10.3.1 Data Backup

Backups are maintained on local servers, on additional multiple servers, on special servers for SFTP and OLAP (current consolidated, historical consolidated, etc.). Process notes for the same are provided in Section 7.3.3.

10.3.2 Power Backup

An Online high-capacity UPS together with an array of batteries can keep the cloud facility running for 8 hours on a full load, in the event of extended power outage.

10.3.3 Internet Service

2 high-speed lines are available at the cloud facility, with the 2nd one serving as a backup for the first.

10.3.4 Hardware

Four standby servers are maintained for ready use, in the event of server failure. All servers are assembled & configured in-house, so a larger number of servers can be replaced or added rapidly if ever needed. Arriba applies a custom-configured OS image based on RHEL derivatives, together with Docker/podman containers. Detailed instructions are documented for all procedures. Any switch-over time would be under 2 hours.

10.3.5 Software backups

Arriba uses the 'subversion' tool for maintaining multiple revisions of team-built software through the development and release process.