

JHA Corporate



Policy

July 2016

## **Third-Party Acceptable Use Policy and Usage Guidelines**

JHA Policy and Guidelines



© 1999 – 2015 Jack Henry & Associates, Inc.

All rights reserved. Information in this document is subject to change without notice. Dates contained in this document are provided as estimates only and can be changed at any time at the sole discretion of Jack Henry & Associates, Inc.

Printed in the United States of America.

No part of this document may be copied, reproduced, stored in a retrieval system, displayed, distributed or transmitted in any form or any means whatsoever (electronic, mechanical or otherwise), including by photocopying or recording for any purpose, without the prior written permission of Jack Henry & Associates, Inc. Making unauthorized copies of this document for any purpose other than your own personal use is a violation of United States copyright laws.

Any unauthorized use of Jack Henry & Associates, Inc.'s trademarks and service marks is strictly prohibited. The following marks are registered and unregistered trademarks and service marks of Jack Henry & Associates, Inc.:

3rd Party Sweep™; 4isight™; Account Analysis™; Account Cross Sell™; Account Cross Sell Jumpstart™; Account Number Change™; ACH/Check Conversion Services™; ACH Client™; ACH Manager™; ACH Origination/Processing™; Advanced Reporting for Credit Unions™; AlertCenter™; AlertManager™; AllAccess™; Alogent®; Alogent® AWARE™; Alogent® Back Counter™; Alogent® Commercial Remote Deposit™; Alogent® Enterprise Duplicate Detection™; Alogent® Front Counter™; Alogent® Image ATM™; Alogent® Interactive Capture™; Alogent® Mobile Remote Deposit™; Alogent® Payment Web Services™; Alogent® Payments Gateway™; Alogent® Remote Deposit Interactive™; Alogent® Retail Remote Deposit™; Andiamo™; Annual Disclosure Statement Online™; ArgoKeys®; ArgoKeys® Branch Sales Automation™; ArgoKeys® DepositKeys™; ArgoKeys® LendingKeys™; ArgoKeys® RelationshipKeys™; ATM Manager Pro®; ATM Manager Pro® – Asset & Site Management™; ATM Manager Pro® – Cash Management™; ATM Manager Pro® – Event Management™; ATM Manager Pro® – Financial Management™; AudioTel™; Banno Mobile™; Basel Report Pro™; BladeCenter™; BondMaster™; Branch Anywhere™; Branch Deposit Reporting Pro™; Brand Management Services™; BusinessManager®; Call Report Pro™; Cash Automation™; Cash Dispenser™; Cash Recycler™; Centurion Business Continuity Planning™; Centurion Business Recovery Consulting Group™; Centurion Co-Location™; Centurion Disaster Recovery®; Centurion Emergency Notification™; Centurion Enterprise-Level Recovery™; Centurion Episys Hosted Failover™; Centurion Hosted High Availability™; Centurion LiveVault™; Check 21 Cash Letter™; Check 21 Exception Processing™; CheckCollectPlus™; Check Collect Recovery Services™; CheckMaster™; CheckMaster Plus™; Check Writer for Core Director®; CIF 20/20®; Co-Mingle™; Cognos 10™; Collateral and Document Tracking™; Commercial Lending Center™; Compliance Access™; Core Director®; Core Director® Teller™; Core Director® Teller Capture™; CreaCard®; Cruise®; CruiseNet®; CTRMaster™; CUPRO® ALM™; CUPRO® ALM Express™; Customer Payment Portal™; Database Cleansing Package™; DataLink CU™; Demand Account Reclassification™; DIME™ (Document Image Management Engagement); DirectLine International™; DirectLine OFX; DirectLine Wires™; Dynamic Content Modules™; ECS Capture Solutions™; ECS Digital Data Conversion™; ECS OneLook™; ECS Paper-to-Digital Conversion™; ECS Web™; eCTR™; Electronic Statements™; Electronic Statements – Interactive™; Enhanced Account Analysis™; Enhanced Loan Application™ (ELA); Enhanced Loan Collections™; Enhanced Member Application™ (EMA); Enterprise Backup and Tape Encryption™; Enterprise Capture Solutions™; Enterprise Conversion Solutions™; Enterprise Payment Solutions™; Episys®; Episys® Anywhere™; Episys® Collateral and Document Tracking™; Episys® Collection Toolkit™; Episys® Contact Event Manager™; Episys® Continuity Plan™ (ECP); Episys® Continuity Services™; Episys® Continuity Services Plus™; Episys® Data Store™; Episys® Dealer Reserve Accounting™; Episys® Escrow Module™; Episys® External Loan Processing Interface™; Episys® Failover Certification™; Episys® Failover Self-Certification™; Episys® ID Scanner Interface™; Episys® Management Server™; Episys® Overdraw Tolerance™; Episys® PowerCheckUp™; Episys® Quest™; Episys® Real Time External Loan Interface™; Episys® Replication Failover™; Episys® Skip Payment™; Episys® University™; Episys® Vaulting™; Episys® Virtualization™; EPS Remote Deposit Capture™; Extra Awards®, Failover™; Fed-File Pro™; FlexPass™; FormsSmart™; Genesys Check Imaging Suite™; Gladiator®; Gladiator® Advanced Malware Protection™; Gladiator® Consulting Services™; Gladiator® CoreDEFENSE Managed Security Services™; Gladiator® eBanking Compliance Services™; Gladiator® eCommercial SAT™; Gladiator® Enterprise Network Design, Implementation & Support Services™; Gladiator® Enterprise Security Monitoring™; Gladiator® Enterprise Virtualization Services™; Gladiator® eSAT™; Gladiator® eShield™; Gladiator® Hosted Network Solutions™; Gladiator® IT Regulatory Compliance/Policy Products™; Gladiator® Managed IT Services™; Gladiator® Managed Unified Communications Services™; Gladiator® NetTeller® Enterprise Security Monitoring™; Gladiator® Network Services™; Gladiator® Phishing Defense and Response Service™; Gladiator® Social Media Compliance Services™; Gladiator® Technology®; Gladiator® Unified Communications Services™; Gladiator® Website Compliance Review™; goDough®; GoldPass™; Hosted Pay Page™; iBizManager™; Image ATM™; Image ATM Capture and Reconciliation™; ImageCenter™; ImageCenter ATM Deposit Management™; ImageCenter Image Capture™; ImageCenter Interactive Teller Capture™; Intellix CIF 20/20® OutLink Renewal Engagement™; Intellix Consulting™; InTouch Voice Response®; Investor Servicing™; iPay Business Bill Pay™; iPay Consumer Bill Pay™; iPay QuickPay™; iPay Solutions™; Isosceles™; iTalk™; Jack Henry & Associates, Inc.®; Jack Henry Banking®; JHA Consumer Pieces™; JHA Get Smart™; JHA Merchant Services™; JHA Money Center™; JHA OutLink Processing Services™; JHA Payment Processing Solutions®; JHA Program Management Services™; JhaAddress Verify™; JhaCall Center™; JhaCall Center In-House™; JhaCall Center Outsourced Services™; JhaCall Center Outsourced Services After Hours™; JhaCall Center Outsourced Full Business Services™; JhaCall Center Outsourced Select Services™; JhaDirect®; JhaEnterprise Workflow™; JhaID Scan™; JhaKnow™; JhaKnow Express™; JhaPassPort Debit Optimizer™; JhaPassPort™; JhaPassPort Pro™; JhaPassPort Direct™; JhaPassPort Extra Awards™; JhaPassPort Fraud Center™; JhaPassPort Hot Card Center™; JhaPassPort Promotions and Consulting Services™; JhaPassPort Switch™; JhaArchive™; JVault®; JXchange™; Kernel™; Know-It-All Credit Programs™; Know-It-All Education™; Know-It-All Learning Management Portal™; Know-It-All Now™; Landlord/Tenant Security Deposit Tracking™; LendingNetwork®; Loan Collateral Tracking™; Margin Maximiser Interactive™; Margin Maximizer Interactive™; Margin Maximiser MaxConnect™; Margin Maximizer MaxConnect™; Margin Maximiser Pronto™; Margin Maximizer Pronto™; Margin Maximiser Suite®, Masterlink™; MaxConnect Interactive™; MedCashManager®; Member Business Services™; Member Privilege™; Mobile Website™; Multifactor Authentication™; Mutual Fund Sweep™; Net.Check™; NetTeller®, NetTeller® Bill Pay™; NetTeller® Cash Management™; NetTeller® MemberConnect™; NetTeller® Online Banking™; NetTeller® Security Manager™; NetTeller® Text Alerts™; OFX Gateway™; OnBoard Loans™; OnNet™; OnTarget™; OnX™; OpCon™; Opening Act™; Opening Act Express™; Optimizer™; Participation Lending™; PassBook™; Point™; PointMobility™; PowerOn®, PowerOn2™; PowerOn Marketplace®; PowerOn Studio™; PPS First PIN™; PPS ImageSelect™; PPS PIN Change Service™; Prepaid Cards™; Professional Consulting Services™; PROFITability®; Organizational PROFITability® Analysis System™; Product PROFITability® Analysis System™; PROFITability® Budget™; PROFITability® Reporting Service™; PROFITstar®; PROFITstar® ALM Budgeting™; PROFITstar® Budget™; PROFITstar® Classic™; PROFITstar® Reporting Service™; ProfitStars®; ProfitStars® Direct™; ProfitStars® EPS SmartPay Business™; ProfitStars® EPS SmartPay Express™; ProfitStars® mRDC™; ProfitStars Synergy®; Real Time™; Refi Analyzer™; Regulatory Reporting Solutions™; Relationship 360™; Relationship Profitability Management™ (RPM); RemitCentral™; RemitPlus®; RemitPlus® Express™; RemitPlus® HRCM™; RemitPlus® Remittance/Lockbox™; RemitWeb™; Remote Deposit Anywhere™; Remote Deposit Complete™; Remote Deposit Express™; Remote Deposit Now™; Remote Deposit Scan™; ReportHub™; RPM Reporting Service™; Shared Branch™; SigMaster™; Silhouette Document Imaging®; SilverLake Real Time™; SilverLake System®; Smart EIP™; Smart GL™; SmartSight®; smsGuardian™; Store & Forward™; StreamLine Platform Automation®; StreamLine Platform Automation® – Deposits™; StreamLine Platform Automation® – Loans™; Summit Support®; Sweep Account Processing™; SymAdvisor™; SymChoice Loan™; SymConnect™; SymForm™; SymForm PDF™; Symitar®; Symitar® ATM Services™; Symitar® Fraud Management™; Symitar® EASE™; SymX™; SymXchange™; Synapsys®; Synapsys® Lobby Tracking™; Synapsys® Member Relationship Management™; Synergy API Integration Toolkit™; Synergy AutoImport™; Synergy Automated Document Recognition™ (ADR); Synergy Batch Document Recognition™ (BDR); Synergy Check Archive™; Synergy DataMart™; Synergy Document Management™; Synergy Document Recognition™; Synergy Document Tracking™; Synergy eDistribution™; Synergy Enterprise Content Management™ (ECM); Synergy eSign™; Synergy eSignWeb™; Synergy eStorage™; Synergy Express™; Synergy ID Scan™; Synergy iSign™; Synergy Kofax Capture™; Synergy PowerSearch™; Synergy Reports™; Synergy Workflow Management™; TellerMaster™; TheWayIPay®; TimeTrack Human Resources™; TimeTrack Payroll System™; TimeTrack Time and Attendance™; Transaction Logging and Vaulting Server™; Transaction Logging Server™; ValuePass™; Vehicle Pricing Interface™; Vertex Teller Automation System™; Vertex Teller Capture™; Virtual Transaction Logging Server™; WebEpisys™; Website Design & Hosting™; Website Security Services™; Wire Management™; Yellow Hammer™; Yellow Hammer ACH Origination™; Yellow Hammer BSA™; Yellow Hammer BSA Regulatory Consulting Service™; Yellow Hammer EFT Fraud Detective™; Yellow Hammer Fraud Detective™; Yellow Hammer SAR Center™; Yellow Hammer Wire Origination™; Xperience™

## Slogans

Cutting-Edge IT Solutions for the Future of Credit Unions™; Know-It-All – Empowering Users Through Knowledge™; Leading through technology ... guiding through support™; Powering Actionable Insight™; Snap it Send it Spend it®; The Depth of Financial Intelligence™; We Are Looking Out For You™; Where Tradition Meets Technology™

Various other trademarks and service marks used or referenced in this document are the property of their respective companies/owners.

Third-Party Acceptable Use Policy and Usage Guidelines.....	1
Usage of JHA Information System Resources .....	1
Guidelines for Usage of JHA Information System Resources .....	2
JHA Information Systems Use Policy .....	2
General.....	2
Internet & JHA Network.....	4
Data & Media .....	5
Telecommunications.....	5
Acknowledgement .....	7

# Third-Party Acceptable Use Policy and Usage Guidelines

## Usage of JHA Information System Resources

All third-party individuals or entities (non-JHA employees) that use or request access to Jack Henry & Associates Information Systems or any of its components must agree to and abide by all parts of the Third-Party Acceptable Use Policy And Usage Guidelines ("Policy"). Third party users can be JHA partners, vendors, suppliers, or temporary labor. This policy applies to all third party entities and includes their employees who will be accessing JHA Information Systems. Reasonable care should be made to ensure all vendors are only given the minimum level of authority. Software vendor support per contract terms acceptable to JHA, in JHA's sole and absolute discretion, may be approved on a per-case-basis by the Director of CIS in place of this form.

Access to various aspects of the system is determined on an "as needed" basis per job function and business necessity. Use of JHA systems is for business purposes only. Any violation of this Policy may result in immediate termination of any partner or other relationship agreement as well as the right to access JHA's information system or any of its components.

- Electronic communications and personal directories must be treated as confidential by users and accessed only by the intended recipient. System users are not authorized to read any messages or information that is not intentionally, clearly, and directly sent to them, and that they maintain a valid contractual right to access.
- System users shall not use a code, access a file or retrieve stored information unless authorized to do so in writing. System users shall not attempt to gain access to another user's messages or directories without the owner's permission. If someone else has accessed a user's password(s), the user must change their password(s) immediately.
- The partner company must notify and receive prior written approval from the appropriate JHA personnel for all configuration or code changes on JHA systems.
- The point of contact for third party users shall notify the JHA HelpDesk in writing when an individual who has access to JHA systems leaves that organization or is transferred to another position that no longer requires access.
- Only employees or agents of the third party who have prior written approval shall use or access JHA resources.
- Third-party users will abide by the security guidelines contained in the Third Party Usage Guidelines described below.
- Third-party users will maintain current contact information with CO – Identity Administration. Users will notify the administrator of any change in contact information, personnel changes, or change in project duration.
- A confidentiality agreement acceptable in form to JHA shall be executed by all parties prior to any grant of access.
- No downloads shall be permitted unless a business need is documented and approved by JHA management in writing.

Visitors to any JHA location enabled with wireless Internet will be offered a Guest Wireless account when they check in with the front desk employees or Security office to get their Visitor badge. Guest Wireless accounts will be created for up to 5 days at a time and access will be for public Internet only. JHA does not guarantee any bandwidth or session duration and Visitors will not be granted access to JHA's corporate network and/or resources. Guest Wireless accounts will work on the majority of mainstream computing equipment, but not phones. Very limited support will be provided to Visitors having trouble connecting to the Guest Wireless due to the vast amount of issues possible with the Visitors' device.

JHA makes no guarantees of protection from electronic attacks, including but not limited to, Denial of Service attacks, viruses, worms, and Trojan Horses. Visitors assume all responsibility for protecting their assets and information from compromise. Attempts to penetrate the JHA networks in any way will be viewed as illegal acts and will be prosecuted to the fullest extent of the law.

## Guidelines for Usage of JHA Information System Resources

Any person using Jack Henry & Associates Information Systems<sup>1</sup> or any of its components must agree to and acknowledge the following:

- Jack Henry & Associates has developed proprietary data processing software, associated products and Information Systems to support the needs of its clients. Access to various aspects of the system is determined on an "as needed" basis by JHA per job function and business necessity.
- The Information Systems may not be used for any illegal activity or activity deemed unethical or inappropriate as defined by this and/or other JHA policies.
- Users of JHA Information Systems are expected to abide by a code of honor to not commit or allow any violation of the tenets of this Policy.
- Any users of JHA Information Systems who violates this Policy or uses the systems for improper purposes shall be subject to immediate termination of access.

Specific policies which must be adhered to are set forth below. JHA reserves the right to change these policies, as required, without notice.

## JHA Information Systems Use Policy

### General<sup>2</sup>

- JHA Information Systems are company property. Additionally, all content composed on, sent from, synced with, downloaded to, or received on JHA Information Systems becomes the property of the company and not the private property of any employee. Any employee composing, sending, syncing, downloading or receiving any content of any nature using JHA Information Systems is subject to having the content intercepted,

---

<sup>1</sup> Information systems – A collection of hardware and software components and interconnections, as well as the information contained within that collection and the facilities that contain and protect them.

<sup>2</sup> Category names are intended only to improve readability and should not be construed to limit the context of any of the policy statements.

recorded, forwarded, reviewed, and/or archived by the company. This includes monitoring telephone calls for business reasons in order to ensure calls are handled in a professional manner and to promote efficiency in the manner in which customers are treated.

- JHA Information Systems are primarily for business use; limited personal use is permitted but must not be excessive or interfere with business needs or operations. Personal use is expected to be on the user's own time and is not to interfere with the person's job responsibilities or access rights.
- JHA Information Systems must not be used or accessed by parties who are not JHA employees, JHA temporary employees, JHA contractors, or others expressly authorized to do so, in writing, by JHA. Any parties accessing or using JHA devices or networks must acknowledge, sign, and adhere to JHA's current Acceptable Use Policy and any necessary confidentiality agreement(s).
- Passwords – Users of JHA Information Systems must not share passwords to or permit use of JHA equipment by members of their households or non-authorized users. Users must not save or store passwords on personal devices (whether manually or using a third-party application) to JHA systems, applications, or products.
- The Information Systems must not be used to communicate or publish improper messages or material, e.g., those that are illegal, defamatory, derogatory, obscene or otherwise inappropriate, including sexually harassing or other offensive messages. Among those which are considered offensive are any messages which contain sexual implications, racial slurs, gender-specific comments, or any other comment that inappropriately addresses someone's age, sexual orientation, religious or political beliefs, national origin, or disability.
- The Information Systems may not be used to solicit, proselytize, support, or maintain messages or material for non-JHA commercial ventures, religious or political causes, outside organizations, or other non-job-related matters, except as approved, in advance writing, by the JHA Legal Department.
- Equipment dedicated to the processing and/or transmittal of financial transactions/data (in particular, machines processing financial transactions on behalf of Customers such as item processing equipment or transaction routing devices), must not be used to access the Internet or have any other usage outside of the equipment's dedicated purpose.
- Users shall not attempt to circumvent the security systems in place on JHA Information Systems or devices and shall not use any code, software, "jail breaking"<sup>3</sup>, hacking tools (ethical or otherwise) to alter, scan, access, or retrieve stored information, nor may any such code, software, "jail breaking," or hacking tools be loaded or utilized on JHA corporate devices, unless authorized in advance writing by the Corporate Security Council.

---

<sup>3</sup> "Jail breaking" can be defined as a smartphone user seeking out a vulnerability and exploiting it. The breaker may use that vulnerability to get root access to the device and then install another operating system, often a version of the original with restrictions removed.



- JHA purchases and/or licenses the use of computer software for business purposes and in some cases does not own the copyright to this software or its related documentation.

Users will not take any actions that would cause JHA to be in breach of any license that JHA has for any third-party software or documentation.

- Users will not keep, use, or distribute any JHA-owned software, information, or the documentation of JHA or any JHA licensee or customer in any fashion in contravention of the work-related purpose of said software, information, or documentation.
- Appropriate Response to Network Threats – If the integrity, in part or in total, of the corporate network(s) is threatened such that the stability, security, and/or functionality of the network or any device is jeopardized, Corporate Services reserves the right to take any and all measures necessary to prevent, or lessen, the effects of the event on JHA and its customers. All reasonable efforts will be made to contact the user/administrator of the device or network prior to, during, and after taking action.

## Internet & JHA Network

- Care should be taken when visiting non-business-related web sites as they have potential risks, viruses, malware, etc.
- Do not use an Internet storage site or third-party webmail (such as Gmail, Hotmail, Yahoo, etc., or ISP webmail such as Suddenlink, Cox, etc.) not approved by Corporate Services for sending, receiving, or storing JHA company or client information.
- Social Media Policy – Third-party users are prohibited from accessing social media using JHA Information Systems.
- Remote Access Policy - Remote Access connections approved by Corporate Services including but not limited to Virtual Private Network (VPN) connections may be granted to users after prior authorization from the user's JHA Contact Manager. These connections will be subject to all authentication and security measures as required by the JHA Communications Department. Access may be revoked at any time for reasons including non-compliance with Acceptable Use or security policies, request by the user's supervisor or negative impact on overall network performance attributable to remote connections. All remote users are expected to strictly abide by all parts of the Acceptable Use Policy.
- Virtual Private Network (VPN) connections other than those approved by Corporate Services are prohibited from use within, or connecting to the network. TOR browsers or any kind of proxy connection software that circumvents monitoring and security measures shall not be installed or used on JHA systems or products, unless authorized by the Corporate Security Council.
- While connected to a wired JHA network connection, you may not also have, on the same device; a concurrent session through a JHA provided device or other wireless, "tethered," or other Internet connection. For example, while connected to a wired JHA



network connection, do not use an “air card” (e.g., Verizon Wireless MiFi) to start a separate Internet session.

- JHA has the capability and reserves the right to track and monitor use of the Internet and its Information Systems.
- The Information Systems must not be used to visit gambling, sexually explicit, offensive, or inappropriate web sites.
- Any and all postings by an employee to social media, blogs, electronic bulletin boards, electronic mailing lists, professional reference sites, forums, and the like, be they public or private, are subject to the Confidentiality Agreement entered into with JHA, prohibiting the release of proprietary information about projects, software products, research and development projects, JHA hardware and device configurations, employee or client information (personally identifiable data such as account number, social security number, name and address, etc.), employed software versions and levels, and all other confidential Jack Henry & Associates, Inc., matters.

## Data & Media

- The JHA corporate e-mail and instant messaging systems are the property of JHA, and all messages composed, sent, or received, and all address book and contact information inputted therein, becomes the property of the company.
- Electronic communications, voicemails, company directories, and personal information stores should be treated as confidential and accessed only by the intended recipient or by authorized personnel as defined by this Policy.
- Internal communications or data (emails, voicemails, files, etc.) regarding JHA personnel, client information, products, services, general business, or any information not yet available in the public domain are not to be forwarded or transmitted outside of JHA systems.
- Data and files containing JHA Corporate or client information must not be stored or backed up using third-party services that are not approved in writing or provided by JHA. (Examples of such disallowed services include but are not limited to Carbonite, CrashPlan, Dropbox, GMail Drive, Windows SkyDrive, and Amazon Simple Storage Service).
- Never send unprotected PANs (Primary Account Number - Credit Card Data) by enduser messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).
- Users of Information Systems may not use any illegal method to obtain or duplicate any media (software, music, movies, etc.) or related documentation on or in connection with JHA Information Systems.
- Users of Information Systems may install business-approved software only. No unauthorized peer-to-peer applications may be installed, including but not limited to BitTorrent, Kazaa, eMule, LimeWire, and uTorrent.
- Instant Messaging Clients and Services – Due to the current technology used by the various third-party Instant Messaging clients and services (for example, Yahoo Messenger, Windows Messenger, AIM, etc.), management has concluded that these

services pose an unacceptable risk to the JHA enterprise. Attempts to send communications via an instant messaging application other than those approved in writing by JHA's Corporate Services (currently Skype for Business) will be treated as a violation of this Policy.

## Telecommunications

- Any personal calls made from JHA offices that result in additional charges billed to JHA may be subject to billing to the User.
- The initiation by users of the recording of telephone calls (other than the routine monitoring of customer calls) is not permitted without the advance written approval of the JHA Legal Department.
- Use of established video conferencing facilities (e.g., J7 presentation rooms) is restricted and must be approved by a set list of JHA personnel that have the ability to reserve the resources. Unless restricted for security or other reasons for specific groups or facilities, desktop web conferencing for business purposes using hardware and software approved and provided by Corporate Services is not prohibited by this Policy.

## Acknowledgement

- Agency/Company: ASPIRE SYSTEMS (INDIA) PVT LTD
- Physical Location: Chennai, India
- Phone: +91 44 6740 4000
- Email: VNATARAJAN@JHACORP.COM
- JHA Project Leader: MITCHELL CLARK
- Estimated duration: 06 MONTHS

I have read and understand this Third Party Acceptable Use Policy and Usage Guidelines and agree to abide by it.

- Name (printed): VIJAYAKUMAR NATARAJAN
- Signature: *N. Vijayakumar*
- Date: 15 June 2021