1.0 INTRODUCTION & SCOPE

1.1 Introduction
1.2 Purpose of the Policy
1.3 Scope of the Document
1.4 Legal Nature of VCQRU's Role
1.5 Definitions
1.6 Application of this Policy
1.7 Acceptance of the Policy

2.0 ROLES & RESPONSIBILITIES (BRAND vs VCQRU)

2.1 Brand Responsibilities
2.2 VCQRU Responsibilities
2.3 Responsibilities VCQRU Does NOT Accept
2.4 Shared Responsibilities
2.5 Liability Framework

3.0 FINANCIAL LIABILITY & FUNDING POLICY

3.1 Financial Responsibility (Brand)
3.2 Pre-Funding Wallet Requirements
3.3 Payout Rules & Approvals
3.4 Failed Payout Liability
3.5 TDS Responsibility
3.6 TDS Funding Requirements
3.7 Budget & Forecasting
3.8 Scheme Financial Accuracy
3.9 Dispute Handling
3.10 Reconciliation Policy
3.11 Non-Financial Liabilities
3.12 Program Pause/Exit Financial Rules
3.13 VCQRU Zero Liability Clause

4.0 TDS, TAXATION & LEGAL COMPLIANCE

4.1 Section 194R Responsibilities
4.2 TDS Deduction
4.3 TDS Deposit
4.4 TDS Return Filing
4.5 Issuing Form 16A
4.6 PAN Collection & KYC Validation
4.7 AML & KYC Compliance
4.8 GST Compliance
4.9 RBI/NPCI Payout Compliance
4.10 Tax Notices & Audit Liability
4.11 Data Retention for Tax
4.12 Payout Reversal & Chargeback Liability
4.13 Penalty Liability

4.14 Indemnification for Tax Issues
4.15 Acknowledgement & Acceptance

5.0 PROGRAM SETUP & SCHEME RULES

5.1 Brand Responsibility for All Scheme Rules
5.2 SKU, Batch & MRP Mapping
5.3 Program Eligibility Rules
5.4 Points Allocation Rules
5.5 Cashback Rules
5.6 Region & Location Restrictions
5.7 User Category Rules
5.8 Fraud Prevention Rules
5.9 Expiry Rules
5.10 Configuration Approval
5.11 Misconfiguration Liability
5.12 Mid-Program Rule Changes
5.13 User Consent & T&C
5.14 Data Reports

6.0 USER VERIFICATION, KYC & ELIGIBILITY

6.1 OTP Login & Identity
6.2 Eligibility Validation
6.3 KYC Requirements
6.4 KYC Approval/Rejection
6.5 Fraud Detection in KYC
6.6 Wrong User Approval Liability
6.7 Blacklisting & Suspension
6.8 Multi-Account & User Abuse
6.9 Document Retention
6.10 Channel Partner Misuse
6.11 Fake Product Users
6.12 Reward Blocking Due to KYC
6.13 Eligibility Dispute Handling
6.14 Verification Audits
6.15 Privacy Consent

7.0 USER DATA HANDLING & PRIVACY

7.1 Types of Data Collected
7.2 Data Minimization
7.3 Data Encryption
7.4 Access Control (RBAC)
7.5 Brand Access Restrictions
7.6 User Consent
7.7 Data Sharing Rules
7.8 Purpose Limitation
7.9 User Rights (Privacy)

7.10 Data Retention & Deletion
7.11 Data Breach Response
7.12 Brand Liability for Misuse
7.13 DPDP/IT Act Compliance

8.0 ANTI-FRAUD, SECURITY & ABUSE CONTROL

8.1 Types of Fraud Detected
8.2 VCQRU's Role
8.3 Brand's Responsibility
8.4 Supply Chain Fraud
8.5 Counterfeit Product Handling
8.6 Internal/Agency Fraud
8.7 Fraud Impact on Payouts
8.8 Anti-Fraud System Features
8.9 Brand Decision-Making
8.10 Wrong/Delayed Action Liability
8.11 Scheme Misuse
8.12 Fraud Indemnity
8.13 Fraud Liability Exclusion

9.0 CUSTOMER SUPPORT & DISPUTE HANDLING

9.1 Brand's Support Ownership
9.2 Complaints Handled by Brand
9.3 VCQRU's Technical Support
9.4 Communication Templates
9.5 Escalation Matrix
9.6 Wrong Reward Disputes
9.7 Product Authenticity Complaints
9.8 Payment/Payout Disputes
9.9 Miscommunication Handling
9.10 Social Media Complaints
9.11 Support Logging
9.12 Final Dispute Liability

10.0 PRODUCT AUTHENTICITY & ANTI-COUNTERFEIT

10.1 Ownership of Authenticity
10.2 Label/QR Data Responsibility
10.3 Label Security
10.4 VCQRU Authentication Role
10.5 Counterfeit Case Handling
10.6 Fake Product Complaints
10.7 Misuse of AC Engine
10.8 Misconfigured Authenticity Logic
10.9 Geo-Based Logic
10.10 Packaging/Label Changes
10.11 Market Scan Spikes

10.12 Legal Liability
10.13 Liability Exclusion

11.0 PROGRAM EXECUTION & CHANGE MANAGEMENT

11.1 Launch Readiness
11.2 Execution Rules
11.3 Content Finalization
11.4 Rule Change Process
11.5 Change Impact Responsibility
11.6 User Communication
11.7 Emergency Changes
11.8 Program Pause/Termination
11.9 Version Control
11.10 Sales Team Miscommunication
11.11 Unapproved Promotions
11.12 Program Execution Liability

12.0 FINANCIAL RECONCILIATION & SETTLEMENT

12.1 Daily Reconciliation
12.2 Weekly Reconciliation
12.3 Monthly Reconciliation
12.4 Reconciliation Failure Liability
12.5 Dispute Resolution
12.6 Failed Payout Handling
12.7 UPI/NEFT Reconciliation
12.8 TDS Reconciliation
12.9 Financial Reports
12.10 Program Closure
12.11 Clearing Dues Before Exit
12.12 Financial Mismatch Liability
12.13 Financial Indemnity

13.0 COMPLIANCE, INDEMNITY & LEGAL PROTECTION

13.1 Regulatory Compliance
13.2 Scheme Legality
13.3 Consumer Protection Compliance
13.4 Indemnity Clause
13.5 Brand Misconduct Liability
13.6 User Claim Exemption
13.7 Limitation of Liability
13.8 Disclaimers
13.9 Force Majeure
13.10 Governing Law
13.11 Dispute Resolution
13.12 Compliance Audits

14.0 TERMINATION, EXIT & DATA HANDLING

14.1 Types of Termination
14.2 Notice Period
14.3 Clearing Dues
14.4 Clearing Payouts
14.5 Handling User Complaints
14.6 Data Handling During Exit
14.7 Data Retention & Deletion
14.8 Post-Termination Compliance
14.9 Immediate Termination Rights
14.10 No Refund Policy
14.11 Intellectual Property
14.12 Termination Certificate

15.0 FINAL ACCEPTANCE & AGREEMENT

15.1 Brand Acceptance
15.2 Signing Authority
15.3 Written Approvals Only
15.4 Entire Agreement Clause
15.5 Modification Rules
15.6 Brand Liability Acceptance
15.7 Liability Cap
15.8 Non-Disparagement
15.9 Confidentiality
15.10 Effective Date
15.11 Renewal
15.12 Jurisdiction
15.13 Signature & Stamping

1.0 INTRODUCTION

This **Brand Onboarding Master Policy** ("Policy") governs the relationship between:

VCQRU Private Limited
("VCQRU", "Technology Provider", "Platform Provider", "We", "Us", "Our")

and

The Brand / Principal Company
("Brand", "Company", "Partner", "Program Owner", "You", "Your")

for the purpose of running:

- Anti-Counterfeit Authentication Programs
- Loyalty / Rewards Programs
- Cashback Schemes (UPI/NEFT)
- Channel Partner Engagement Programs
- Consumer Awareness Campaigns
- KYC-based reward schemes
- Product traceability systems

VCQRU is an **independent technology provider**, not a manufacturer, seller, or reward issuer.

This policy clearly defines:

✔ VCQRU's role (Technology Only)
✔ Brand's responsibilities (End-to-End Legal + Financial + Compliance)
✔ Data boundaries and rules
✔ Financial liability, TDS responsibility, and tax responsibility
✔ Reward and cashback responsibility
✔ AC (Anti-Counterfeit) logic and brand accountability
✔ System usage rules
✔ Indemnity, security, and compliance requirements

The brand **must read, accept, and sign this policy** before launching any scheme.

1.1 PURPOSE OF THE POLICY

The purpose of this policy is to:

1. Clearly establish legal, operational, financial, and compliance responsibilities
2. Protect VCQRU from liabilities arising from brand programs
3. Ensure brands comply fully with all laws and tax obligations
4. Maintain system integrity, user trust, and fairness
5. Prevent misuse, fraud, and operational gaps
6. Ensure correct onboarding, setup, maintenance, and closure of programs
7. Define clear expectations from the Brand

This document becomes part of:

✔ The Master Service Agreement (MSA)
✔ Product/Project Agreement
✔ Legal Annexures
✔ Data Protection Addendum
✔ SOP Manuals
✔ Tax & Finance Compliance Framework

1.2 SCOPE OF THE DOCUMENT

This policy applies to **all services** provided by VCQRU to the Brand under:

✔ Anti-Counterfeit (AC) Programs

- QR code scanning
- Security code validation
- Real-time authenticity results
- Duplicate scan alerts
- Counterfeit risk analytics
- Traceability and batch mapping

✔ Build Loyalty (BL) Programs

- Points allocation
- Cashback rewards
- UPI/NEFT payouts
- Earn & burn rules
- KYC management
- Ledger management
- Payout retries

✔ Program Activation & User Management

- User onboarding
- User login with OTP
- KYC workflow
- Eligibility enforcement
- Fraud detection

✔ Platform Access & Technical Infrastructure

- Web portals
- Admin dashboards
- Mobile-web pages
- APIs
- Fraud engines
- Real-time notification engines

✔ Data Management & Security

- Data encryption
- Secure storage
- Access control
- Data usage rules
- Data retention

✔ Taxation, TDS, Finance & Reporting

(covered in detail in Batch 4)

1.3 LEGAL NATURE OF VCQRU'S ROLE

VCQRU acts **only as a Technology Platform Provider** offering:

- Software-as-a-Service (SaaS)
- Anti-counterfeit authentication engine
- Loyalty and reward management system
- Communication engine (SMS/WhatsApp, etc.)
- UPI/Bank payout processing engine
- Fraud detection algorithms
- Analytics dashboards
- User management modules
- KYC workflow tool

VCQRU is **NOT**:

❌ A reward issuer
❌ A product manufacturer
❌ A seller or distributor
❌ A payment guarantor
❌ A tax deductor or tax filer
❌ A legal custodian of brand obligations
❌ Responsible for consumer disputes
❌ Responsible for counterfeit product handling
❌ Responsible for wrong KYC or wrong payout decisions

The brand **bears FULL responsibility**, always.

1.4 DEFINITIONS (BRAND-SPECIFIC)

Brand

A legal entity/manufacturer/organization that uses VCQRU technology.

Program

Any reward, loyalty, anti-counterfeit, or awareness scheme launched by the Brand.

User

A consumer, dealer, distributor, mechanic, electrician, carpenter, painter, retailer, or partner who scans codes or claims rewards.

Reward

Any financial or non-financial benefit such as cashback, points, vouchers, gifts, or merchandise.

Cashback

UPI or bank transfer processed to the user based on brand-defined rules.

KYC

Identity verification required by the brand, including PAN, Aadhaar, license, GST, or other documents.

Fund Wallet

Reward/cashback fund deposited by the brand with VCQRU's payout partner for disbursement.

AC Engine

VCQRU's anti-counterfeit authentication module.

BL Engine

VCQRU's build loyalty and rewards module.

1.5 APPLICATION OF THIS POLICY

This policy applies to:

✔ All new brands onboarded
✔ All renewal programs
✔ All pilot programs
✔ All channels (web, app, QR, chatbot)
✔ All users participating in the scheme
✔ All units (SKU/Batches) mapped to the program
✔ All payout and reward actions

This policy is **binding** on:

- Brand's management team
- Brand's marketing team
- Brand's finance and tax team
- Brand's channel & sales team
- Any third party assigned by the brand

1.6 ACCEPTANCE OF THE POLICY

By onboarding on VCQRU's platform, the brand agrees that:

1. VCQRU is only a **technology provider**
2. All legal, financial, tax, and compliance responsibility lies on the brand
3. VCQRU has no liability for product or scheme issues
4. Brand will indemnify VCQRU for any claims arising from:
    - Product defects
    - Counterfeit issues
    - Wrong payouts
    - Tax non-compliance
    - KYC errors
    - User disputes
    - Regulatory issues
    - Misuse or fraud

This acceptance must be:

✔ Signed physically or digitally
✔ Part of the master agreement
✔ Acknowledged by brand's authorized signatory

2.0 OVERVIEW

This section clarifies the responsibilities of:

- **The Brand (Program Owner)**
- **VCQRU (Technology Provider)**

The Brand is the **full legal owner** of the anti-counterfeit program, loyalty program, or cashback scheme.

VCQRU is the **platform provider only**, not the issuer or beneficiary provider.

2.1 BRAND RESPONSIBILITIES (FULL LIST — LEGALLY BINDING)

The following responsibilities belong ENTIRELY and EXCLUSIVELY to the Brand.

This section must be included in the brand contract.

2.1.1 Product Data Responsibility

Brand must ensure:

✔ All SKU data is correct
✔ Batch mapping is correct
✔ QR or label data is correct
✔ No duplication in product codes
✔ No wrong expiry/MRP/batch uploads
✔ Correct activation/deactivation of SKUs

❗ **VCQRU is NOT liable for:**

- Wrong data uploaded
- Incorrect batch information
- Faulty code series

Brand bears 100% liability.

2.1.2 Program Rules & Scheme Logic

Brand must define:

✔ Eligibility criteria
✔ Point slabs
✔ Cashback slabs
✔ Channel partner rules
✔ Geography limitations
✔ KYC requirement
✔ Maximum earning rules
✔ Fraud/Penalty rules
✔ Approval/rejection rules
✔ Reward expiry logic

VCQRU executes logic EXACTLY as defined.

❗ **VCQRU is NOT responsible for:**

- Wrong rules
- Missing rules
- Confusing rules
- User dissatisfaction caused by brand rules

2.1.3 Fund Management & Budget Liability

Brand must ensure:

✔ Program is adequately funded
✔ Wallets have sufficient balance
✔ Payout reserves are maintained
✔ Fund transfers to payout partner are timely
✔ No bounced transactions

❗ **VCQRU has ZERO liability for:**

- Insufficient brand funds
- Payment failures due to fund shortage
- User complaints caused by no budget

All liabilities fall on the brand.

2.1.4 KYC Verification Responsibility

Brand must:

✔ Decide if KYC is needed
✔ Define KYC rules
✔ Approve/reject KYC
✔ Verify authenticity of documents
✔ Maintain compliance

VCQRU only provides workflow — not approval.

2.1.5 TDS, Tax & Compliance Liability (MOST IMPORTANT)

Brand is FULLY responsible for:

✔ Deducting TDS under 194R
✔ Depositing TDS to govt
✔ Filing TDS returns (26Q)
✔ Issuing Form 16A
✔ Maintaining PAN/KYC data
✔ Handling tax disputes

VCQRU has ZERO tax responsibility.

2.1.6 Product Quality, Warranty, Replacement & Refund

Brand is responsible for ALL product-related matters:

✔ Replacements
✔ Warranty
✔ Refunds
✔ Safety issues
✔ Health issues
✔ Manufacturing defects

VCQRU has no involvement.

2.1.7 Handling Fake Product Complaints

Brand must manage:

✔ Customer complaints
✔ Product returns
✔ Investigations
✔ Legal action
✔ Retailer/distributor misconduct

VCQRU only provides scan results based on brand's data.

2.1.8 User Communication & Customer Support

Brand must provide:

✔ Customer care support
✔ Toll-free numbers
✔ Email support
✔ Complaint escalation process
✔ Resolution of user disputes

VCQRU supports ONLY technical issues.

2.1.9 Legal Liability & Indemnification

Brand must indemnify VCQRU against:

✔ User disputes
✔ Product claims
✔ Tax notices
✔ Government audits
✔ Consumer court cases
✔ Manufacturer liabilities
✔ Distributor/retailer disputes
✔ Reward disputes

VCQRU must never be made liable.

2.1.10 Ensuring Correct Audience Uses the Program

Brand must ensure:

✔ Genuine mechanics, electricians, painters, carpenters, dealers, retailers, etc.
✔ No fraudulent or unqualified participants
✔ No misuse via third parties
✔ Correct internal distribution to channel partners

VCQRU does not manage qualification.

2.2 VCQRU RESPONSIBILITIES (TECHNOLOGY ONLY)

VCQRU is responsible ONLY for platform, technology, and security.

2.2.1 Platform Availability & Technical Uptime

VCQRU ensures:

✔ Stable platform
✔ QR scanning engine
✔ Loyalty engine
✔ Analytics dashboard
✔ OTP login
✔ Secure user portal

2.2.2 Data Security & Encryption

VCQRU ensures:

✔ Secure storage (AES-256)
✔ Role-based access
✔ Data masking
✔ VPN/block detection
✔ Fraud engine
✔ Activity logs
✔ Backups

2.2.3 Execution of Brand Logic

VCQRU executes:

✔ Scheme logic
✔ Points logic
✔ Cashback logic
✔ KYC workflow
✔ Payout processing

Exactly as defined by brand.

2.2.4 Technical Customer Support

VCQRU handles:

✔ OTP issues
✔ Scanning issues
✔ Portal access issues
✔ Platform bugs
✔ Payment technical errors

NOT product disputes.

2.2.5 Fraud Detection & Flagging

VCQRU provides:

✔ Duplicate scan detection
✔ GPS/VPN abuse detection
✔ Multi-account detection
✔ Device fingerprinting
✔ Repeat fraud alerts

Brand must act on flagged data.

2.3 RESPONSIBILITIES VCQRU DOES *NOT* ACCEPT (FULL LEGAL PROTECTION)

This section protects VCQRU from all liability.

VCQRU is NOT responsible for:

❌ Product quality
❌ Wrong batch/QR data
❌ Retailer/distributor misuse
❌ Fake product incidents
❌ Counterfeit market actions
❌ Reward eligibility decisions
❌ Reward approval/rejection
❌ Incorrect payouts due to brand rules
❌ Insufficient program funds
❌ Wrong data uploaded by brand
❌ KYC approval errors
❌ TDS or tax issues
❌ Legal disputes from users
❌ Return/refund/warranty
❌ Scheme miscommunication
❌ Delayed reward announcements

These are 100% brand responsibility.

2.4 SHARED RESPONSIBILITIES (CLEAR-BOUNDARIES)

Some activities require cooperation:

✔ Fraud prevention

VCQRU detects → Brand takes action

✔ Program execution

VCQRU runs logic → Brand reviews results

✔ Customer resolution (technical + program)

VCQRU handles tech → Brand handles program disputes

✔ **Program change management**

Brand approves → VCQRU implements

2.5 LIABILITY FRAMEWORK (CRITICAL)

This defines who is responsible if something goes wrong.

A) Financial Liability → BRAND

All payouts, TDS, KYC issues, reward disputes = **Brand liability**.

B) Legal Liability → BRAND

Product, counterfeit, user complaints = **Brand liability**.

C) Data Security Liability → VCQRU

Storage, encryption, security = **VCQRU responsibility**.

D) Fraud & Abuse Liability → BRAND

User misuse, multi-account abuse = **Brand must handle** with our data.

E) Program Failure Due to Brand Errors → BRAND

Wrong rules, wrong data, insufficient funds = **Brand liability**.

3.0 OVERVIEW

This section defines:

✔ Who pays for rewards
✔ Who is financially liable for payouts
✔ Who manages TDS
✔ Who funds the wallet
✔ Who handles reconciliation
✔ Who is responsible for user complaints
✔ What happens if the brand has insufficient funds
✔ Why VCQRU is NEVER liable for payout failures

The purpose is to protect VCQRU from ALL financial risks.

3.1 BRAND IS 100% FINANCIALLY RESPONSIBLE FOR ALL PAYOUTS

The Brand agrees and acknowledges that:

VCQRU IS NOT a wallet holder, bank, finance entity, or reward issuer.

VCQRU ONLY triggers payouts on behalf of the Brand using Brand-funded accounts.

Therefore:

All loyalty rewards, cashback, points, and benefits are 100% funded, owned, and operated by the Brand.

VCQRU does NOT:

❌ Pay any rewards
❌ Issue cashback
❌ Maintain reward liabilities
❌ Guarantee payments
❌ Bear loss due to wrong payouts
❌ Carry any outstanding liability
❌ Lend money for rewards

3.2 BRAND MUST PRE-FUND THE WALLET / PAYOUT ACCOUNT

Before launching the program, the Brand must:

✔ Deposit required funds into the payout partner wallet (UPI/NEFT)
✔ Maintain running balance
✔ Ensure zero shortfall
✔ Top-up wallet immediately when balance is low
✔ Provide payout reserve as per expected daily volume

VCQRU WILL NOT process payouts if funds are insufficient.

VCQRU is protected from:

- Delays caused by insufficient funds
- User complaints
- Financial liability
- Penalties

3.3 NO PAYOUT OR POINT ISSUANCE WITHOUT BRAND APPROVAL

VCQRU only follows rules configured by the Brand.

Every reward, points, cashback, or payout is:

✔ Calculated based on Brand rules
✔ Approved by Brand logic
✔ Issued only after Brand wallet has money

VCQRU has **zero discretionary power**.

3.4 BRAND LIABILITY FOR FAILED PAYOUTS

If payout fails due to:

- Wrong UPI entered by user
- Wrong bank details
- User account closed
- Bank downtime
- UPI server error
- Low brand wallet balance
- Brand's internal approval delay
- Compliance hold (KYC/PAN mismatch)
- Limit breach by user

Brand is fully responsible for resolution & reprocessing.

VCQRU is NOT responsible for:

❌ Payment reversals
❌ Refunding users
❌ User dissatisfaction
❌ Complaints in Play Store/Social Media

3.5 BRAND IS RESPONSIBLE FOR MANAGING TDS (Under Section 194R)

Brand must:

✔ Calculate TDS
✔ Deduct TDS
✔ Deposit TDS
✔ Issue TDS certificates
✔ File returns
✔ Handle tax disputes

VCQRU only displays tax values *as provided by the Brand*.
VCQRU has **0 tax liability**.

3.6 BRAND MUST FUND TDS AMOUNTS SEPARATELY (IF APPLICABLE)

If TDS is deductible:

- Brand must deposit tax amount
- VCQRU cannot adjust TDS from own funds
- Brand must maintain separate TDS reserve

VCQRU will NOT:

❌ Advance TDS
❌ Pay tax on Brand's behalf
❌ Bear penalty for missed tax filing

3.7 BRAND RESPONSIBLE FOR PROGRAM BUDGET & FINANCIAL PLANNING

Brand must plan:

✔ Expected scan volume
✔ Expected reward distribution
✔ Monthly fund requirements
✔ Maximum payout limits
✔ Seasonal demand spikes
✔ Scheme abuse impact

VCQRU is not responsible for:

❌ Budget shortage
❌ Over-redemption by users
❌ Incorrect financial forecasting

3.8 VCQRU NOT LIABLE FOR INCORRECT SCHEME FINANCIALS

If the Brand sets:

- Wrong reward value
- Wrong conversion rate
- Wrong point slab
- Wrong cashback formula
- Mistakenly high payout rules

The Brand absorbs the loss — NOT VCQRU.

VCQRU executes EXACTLY what Brand configures.

3.9 FINANCIAL DISPUTE HANDLING (BRAND'S DUTY)

The Brand must handle all financial disputes raised by users, such as:

- "I did not receive cashback"
- "UPI sent to wrong account"
- "Less cashback credited"
- "Points not correct"

- “Reward not approved”
- “Tax deducted wrongly”

VCQRU provides logs ONLY — not decision-making.

3.10 RECONCILIATION POLICY

Brand must perform:

✔ Daily transaction reconciliation
✔ Weekly payout reconciliation
✔ Monthly TDS reconciliation
✔ Quarterly reward ledger review

VCQRU provides:

✔ Logs
✔ APIs
✔ Dashboards

But **brand must close reconciliation**.

3.11 NON-FINANCIAL LIABILITIES RELATED TO USERS

Brand is solely responsible for:

- User onboarding
- Ensuring correct audience (mechanics/retailers/etc.)
- Handling user disputes
- Ensuring KYC compliance
- Avoiding wrongful payments
- Monitoring channel partner misuse

VCQRU is not responsible for wrong beneficiaries.

3.12 SAFE EXITS, PAUSES & PROGRAM TERMINATION

If brand stops or pauses the program:

✔ All outstanding payouts must be cleared
✔ Brand must notify all users
✔ Brand must settle remaining liabilities
✔ Brand must bear legal responsibility for unsettled claims

VCQRU will not:

❌ Clear pending payouts
❌ Handle user anger
❌ Manage refunds or liabilities

3.13 VCQRU HOLDS ZERO FINANCIAL LIABILITY

This is the most important legal clause.

The brand acknowledges that:

VCQRU holds absolutely NO liability for any:

- Reward
- Cashback
- Payout
- KYC
- Tax
- Fund shortage
- Scheme abuse
- User dispute
- Government penalty
- Loss due to brand configurations
- Wrong SKU mapping
- Wrong UPI entered by user
- Duplicate payout
- Unpaid user benefits

Brand indemnifies VCQRU against ALL financial claims.

4.0 OVERVIEW

This section defines **all tax-related responsibilities**, including:

- TDS under Section 194R
- PAN collection
- KYC compliance
- GST
- AML (Anti-Money Laundering)
- Regulatory reporting
- Government audits
- Legal notices
- Penalties

100% of ALL tax-related responsibilities lie with the Brand ONLY.

VCQRU will **never deduct, deposit, manage, or file taxes** on behalf of any Brand.

4.1 SECTION 194R – BRAND'S FULL & UNDIVIDED RESPONSIBILITY

Section 194R of the Income Tax Act mandates **TDS on all benefits and perquisites** offered to users such as:

- Cashback

- Points converted to cash
- Gift vouchers
- Free products
- Rewards
- Incentives to channel partners (mechanics, electricians, dealers, retailers, etc.)

Therefore, the Brand agrees and acknowledges:

****VCQRU IS NOT the "provider of benefit or perquisite".**

VCQRU IS NOT responsible for deducting or depositing TDS.
VCQRU IS NOT liable for tax disputes, audits, notices, penalties.**

The Brand, and the Brand alone, is 100% responsible for Section 194R compliance.

4.2 TDS Deduction Responsibility (Brand Only)

The Brand must:

✔ Deduct correct TDS on every eligible reward
✔ Apply higher TDS if PAN is missing
✔ Maintain threshold calculations (₹20,000/₹5,000 as applicable)
✔ Maintain user-wise TDS records
✔ Store and audit user PAN & KYC
✔ Notify VCQRU about deduction rules
✔ Ensure timely deduction

VCQRU simply executes payouts **AFTER** TDS instructions from the Brand.

4.3 TDS Deposit Responsibility (Brand Only)

Brand must deposit deducted TDS:

✔ Within statutory deadlines
✔ Through authorized channels
✔ In correct government challans
✔ With correct PAN, section code, nature of payment
✔ Without error

VCQRU does not:

❌ Deposit TDS
❌ Validate deposits
❌ Maintain challan records

4.4 TDS Return Filing Responsibility (Brand Only)

Brand must file periodic returns including:

✔ Form 26Q
✔ Quarterly returns
✔ Correction returns
✔ TDS reconciliation statements

VCQRU does not and will not:

❌ File returns
❌ Reconcile TDS
❌ Manage update/correction requests

4.5 Issuing TDS Certificates (Form 16A)

Brand must:

✔ Issue Form 16A to all beneficiaries
✔ Issue timely and accurate certificates
✔ Manage rectifications
✔ Handle user complaints

VCQRU is not involved in TDS certificate generation.

4.6 PAN Collection & Validation Responsibility

Brand must:

✔ Decide if PAN is mandatory
✔ Collect PAN
✔ Validate authenticity of PAN
✔ Store PAN securely
✔ Ensure compliance with tax laws

If PAN is invalid, user is ineligible OR higher TDS is required.

VCQRU's role is limited to:

✔ Storing PAN in encrypted format
✔ Providing PAN upload workflow

The Brand is legally responsible for correctness.

4.7 KYC & AML (Anti-Money Laundering) Compliance

Brand must ensure:

✔ Mandatory KYC (if required)
✔ KYC authenticity (no fake documents)
✔ AML checks for high-value users

✔ Record-keeping for compliance
✔ Verification of identity before payout

VCQRU provides the technical platform ONLY.

4.8 GST Responsibility (Brand Only)

If the Brand chooses to offer:

- Goods
- Coupons
- Vouchers
- Physical gifts
- Merchandise

Brand must:

✔ Handle GST valuation
✔ File GST returns
✔ Maintain HSN codes
✔ Issue invoices (if required)
✔ Manage GST disputes

VCQRU cannot and will not advise on GST or handle GST filings.

4.9 Compliance with RBI/NPCI Payout Regulations

For UPI/NEFT payouts:

Brand must ensure:

✔ Compliance with UPI payout norms
✔ Monitoring of suspicious payouts
✔ Daily reconciliation
✔ No payout to blocked/illegal users
✔ Validation of UPI/bank accounts

VCQRU only triggers payments through authorized payout partners.

4.10 Full Legal Liability for Tax Notices, Audits & Investigations

If ANY of the following occur:

- Income Tax notice
- TDS audit
- GST audit
- AML investigation
- Reward misuse probe
- Consumer court notice

The Brand is SOLELY responsible.

VCQRU is indemnified against ALL such liabilities.

4.11 Data Retention for Tax Compliance

Brand is responsible for:

✔ Maintaining KYC & PAN documents for the legal period
✔ Keeping a record of user payouts
✔ Maintaining audit logs
✔ Responding to tax notices

VCQRU only retains data for the duration legally required and does not manage government interactions.

4.12 Payout Reversal, Chargeback & Refund Responsibility

If payouts fail or require reversal due to:

- Wrong UPI entered by user
- Bank rejects credit
- User claims incorrect amount
- TDS mismatch
- Government inquiry

Brand must:

✔ Handle all such cases
✔ Perform manual or automated reprocessing
✔ Bear any financial loss

VCQRU is not liable for reversals.

4.13 Penalty Liability (Brand Only)

If penalties arise due to:

- Late TDS deposit
- Wrong TDS deduction
- Incorrect PAN
- Wrong threshold logic
- Incorrect filing
- GST noncompliance
- AML violations
- Wrong payout to incorrect user
- Reward misuse due to brand’s eligibility logic

Brand accepts FULL liability.

VCQRU is indemnified.

4.14 Legal Indemnification Clause for All Taxation Issues

The Brand agrees that:

All tax obligations, penalties, disputes, errors, notices, audits, refunds, interests, and assessments are the BRAND'S FULL AND EXCLUSIVE responsibility.

VCQRU shall not be responsible or liable for any tax or legal claims under ANY circumstances.

Brand indemnifies VCQRU against ALL tax risks arising from:

- Cashback
- Points
- Rewards
- Product giveaways
- TDS errors
- Non-compliance
- Fraudulent KYC
- Wrong beneficiary payouts

4.15 Acknowledgement & Acceptance

The Brand formally acknowledges:

✔ VCQRU is a *technology provider only*
✔ Brand is the *benefit provider*
✔ Brand is the *tax deductor & depositor*
✔ All 194R responsibility lies with the Brand
✔ All payout liability lies with the Brand
✔ All user-facing issues are Brand's responsibility
✔ Brand fully indemnifies VCQRU

Digital signature/contract sign-off confirms acceptance.

5.0 OVERVIEW

This section defines the complete structure and responsibilities related to:

- Program logic
- Eligibility criteria
- Reward/point/cashback rules
- SKU & Batch mapping
- Approval workflows
- Region/role-based targeting
- Duplicate handling
- Rule changes during a live campaign

- Expiry and limit rules

5.1 BRAND RESPONSIBILITY FOR DEFINING ALL SCHEME RULES

The Brand acknowledges that **ONLY the Brand** is authorized and responsible for:

✔ Designing the scheme
✔ Defining slabs
✔ Setting point values
✔ Setting cashback amounts
✔ Defining payouts
✔ Setting user categories
✔ Approving reward logic
✔ All eligibility criteria
✔ All reward conditions

VCQRU implements the rules **exactly as provided**.

VCQRU is NOT responsible for:

- Wrong decisions taken by Brand
- Wrong calculations provided by Brand
- User dissatisfaction due to Brand’s scheme design
- Misaligned reward structure

5.2 SKU, BATCH, MRP & EXPIRY MAPPING (Brand Only)

Brand must ensure:

✔ Correct SKU codes
✔ Correct batch numbers
✔ Correct MRP values
✔ Correct expiry dates
✔ Correct mapping of batches to slabs
✔ Correct activation/deactivation of SKUs
✔ No duplicate batches
✔ No cross-mapped SKU issues

VCQRU is NOT responsible for:

- Wrong SKU mapping
- Fake alerts due to incorrect batch uploads
- Incorrect product-level eligibility
- Any loss due to wrong data uploaded

Brand is fully liable for errors.

5.3 PROGRAM ELIGIBILITY RULES (Brand Must Define)

Brand must define eligibility, including:

- Product eligibility
- Market/Region eligibility
- User type (mechanic/retailer/consumer/etc.)
- Minimum/maximum scans
- Maximum redemption
- Daily/weekly/monthly earning limits
- Participation restrictions

VCQRU will NOT decide eligibility.

5.4 POINTS ALLOCATION RULES (Brand Only)

Brand must specify:

✔ How many points per scan
✔ For which SKU
✔ For which location
✔ For which user type
✔ Daily/weekly caps
✔ Multi-scan caps
✔ Geo-restrictions
✔ Validity period
✔ Expiry rules

VCQRU does NOT modify point logic.

5.5 CASHBACK RULES (Brand Only)

Cashback conditions must be defined by the Brand:

✔ Cashback amount
✔ Cashback triggering criteria
✔ Min/Max payout limits
✔ KYC-linked cashback rules
✔ TDS-linked rules
✔ Threshold limitations
✔ Cashback expiry
✔ Reversal conditions

VCQRU is NOT liable for any installment, cap, or rule mismatch.

5.6 REGION & LOCATION RESTRICTION RULES

The Brand must define:

- Allowed states
- Allowed districts

- Allowed pin codes
- Restricted zones
- Channel-specific regions

VCQRU uses location data only for rule enforcement.

5.7 USER CATEGORY & ROLE-BASED RULES

Brand must define the following role categories:

- Mechanic
- Electrician
- Plumber
- Carpenter
- Painter
- Retailer
- Distributor
- Consumer
- Dealer
- Technician

Brand must determine:

✔ Eligibility of each role
✔ Reward rules per category
✔ Caps & restrictions
✔ KYC requirements per category

VCQRU will NOT classify users.

5.8 FRAUD PREVENTION RULES (Brand Must Approve)

Brand must define:

✔ Duplicate scan rules
✔ Max scans per batch
✔ Max scans per day
✔ Allowed scan intervals
✔ Fraud penalty (points/cashback reversal)
✔ Blacklisting criteria
✔ Re-verification criteria

VCQRU provides detection → Brand decides action.

5.9 EXPIRY RULES FOR REWARDS, SCANS & POINTS

Brand must define expiry duration for:

✔ Points
✔ Cashback eligibility
✔ Scan results
✔ KYC validity
✔ Reward validity

VCQRU automatically enforces expiry rules **as configured by the Brand**.

5.10 PROGRAM CONFIGURATION APPROVAL

Before going live:

Brand must approve:

✔ Scheme SOP document
✔ Final program rules
✔ Final slab chart
✔ Final SKU/Batches mapping
✔ Final payout logic
✔ All conditional logic
✔ All TDS rules
✔ All KYC rules
✔ All user-facing text
✔ Terms & Conditions

VCQRU will NOT launch a program without explicit Brand approval.

5.11 BRAND RESPONSIBLE FOR MISCONFIGURATIONS

If Brand provides:

- Wrong logic
- Wrong formulas
- Wrong mapping
- Wrong eligibility rules
- Wrong payout structure
- Incorrect TDS rules
- Faulty conditions
- Over-generous slabs

Brand absorbs all financial and legal liability.

VCQRU is NOT responsible for:

❌ Extra payouts
❌ Wrong rewards
❌ Over-redemption
❌ Fraud loss due to poor rule design

5.12 RULE CHANGES DURING LIVE PROGRAM

If Brand wants to change rules:

Brand must:

✔ Provide written request
✔ Approve impact analysis
✔ Accept financial impact
✔ Communicate rule changes to users
✔ Accept legal responsibilities for change

VCQRU only implements changes technically.

5.13 USER CONSENT & ACCEPTANCE (Brand Must Provide Text)

Brand must provide:

✔ Terms & Conditions
✔ Reward rules
✔ KYC rules
✔ Cashback rules
✔ Eligibility
✔ Fraud rules
✔ Disclaimer

VCQRU will not write or own Brand T&Cs.

5.14 DATA REPORTS & ANALYTICS CONFIGURATION

Brand must define:

✔ KPIs
✔ Metrics
✔ Report format
✔ Dashboard requirements
✔ Daily/weekly reporting

VCQRU will configure as per brand requirement.

6.0 OVERVIEW

This section defines:

- How users are verified
- Who decides eligibility
- Who approves/rejects KYC
- Who ensures correct audience (mechanic/retailer/etc.)
- Brand liabilities for wrong approvals

- Fraud & misuse controls

VCQRU provides only the **technical system**, while the Brand owns **all decisions**.

6.1 USER IDENTITY VERIFICATION (OTP Login)

All users access the program using:

✔ Mobile number OTP (SMS/WhatsApp)
✔ Optional UPI verification
✔ Optional email OTP

VCQRU ensures:

✔ Secure OTP gateway integration
✔ Authentication logs
✔ Fraud detection signals

Brand is responsible for:

- Accepting OTP as legal user identity
- Handling disputes related to identity
- Ensuring mobile numbers are correct

VCQRU DOES NOT validate user identity beyond OTP.

6.2 BRAND RESPONSIBILITY FOR USER ELIGIBILITY VALIDATION

Brand must define:

✔ Who is eligible
✔ Who is NOT eligible
✔ What disqualifies a user
✔ What documents prove eligibility
✔ How user category is verified

Examples of eligibility types:

- Mechanics
- Electricians
- Carpenters
- Plumbers
- Painters
- Retailers
- Dealers
- Farmers
- Distributors
- Consumers

VCQRU DOES NOT classify or verify user type.

6.3 KYC REQUIREMENT (Brand Must Decide)

Brand must define:

✔ Whether KYC is required
✔ What type of documents are valid
✔ What data is necessary (PAN, Aadhaar, etc.)
✔ Whether face-match or OCR is required
✔ KYC approval criteria
✔ KYC rejection criteria

VCQRU will provide the **technical KYC workflow** only.

✔ VCQRU DOES NOT approve or reject KYC

✔ VCQRU DOES NOT validate authenticity of documents

✔ VCQRU DOES NOT perform compliance checks

All approvals are BRAND responsibility.

6.4 BRAND RESPONSIBILITY FOR KYC APPROVAL & REJECTION

Brand must:

✔ Verify documents uploaded by the user
✔ Confirm authenticity
✔ Ensure PAN belongs to the same user
✔ Check images are real and unedited
✔ Validate Aadhaar info (if used)
✔ Ensure KYC meets legal requirements

If the Brand approves a fake or incorrect KYC:

→ 100% liability is on the BRAND
→ VCQRU will NOT handle penalties
→ VCQRU is indemnified

6.5 FRAUD DETECTION IN KYC (Brand Must Act)

VCQRU can detect and flag suspicious behavior:

✔ Same PAN used across multiple accounts
✔ Same Aadhaar used by multiple users
✔ Manipulated documents
✔ Blacklisted mobile/device
✔ Abnormal location changes

VCQRU only **alerts**.

Brand must:

✔ Investigate
✔ Decide action
✔ Reject/blacklist user
✔ Inform the user

VCQRU is not responsible for enforcement.

6.6 RESPONSIBILITY FOR WRONG USER APPROVAL

If the Brand mistakenly approves:

- Wrong user category
- Fake mechanic
- Wrong retailer
- Fraudulent participants
- Dealer pretending to be consumer
- Distributor scanning products meant for consumers

The Brand is fully responsible.

VCQRU carries **zero liability**.

6.7 BLACKLISTING & SUSPENSION RULES (Brand Must Define)

Brand must define:

✔ Who can be blacklisted
✔ What activity qualifies as fraud
✔ Appeal process (if any)
✔ Permanent or temporary restrictions
✔ Rules for unblocking

VCQRU only executes blacklist after brand instruction.

6.8 USER MISUSE & MULTI-ACCOUNT ABUSE

Brand is responsible for defining:

✔ Account linking rules
✔ Multi-device restrictions
✔ Device fingerprint rules
✔ Same UPI misuse
✔ Same PAN misuse
✔ Location spoofing
✔ GPS fraud
✔ VPN abuse

VCQRU detects — Brand acts.

6.9 USER DOCUMENT & DATA RETENTION RULES

Brand must legally comply with:

✔ PAN storage rules
✔ KYC retention rules
✔ AML document retention
✔ GDPR/DPDP compliance
✔ Data destruction after legal retention period

VCQRU provides secure storage only.

Brand owns compliance obligations.

6.10 RESPONSIBILITY FOR CHANNEL PARTNER MISUSE

If product codes are misused by:

- Distributors
- Retailers
- Dealers
- Sales teams
- Field agents
- Warehouse teams

Brand is responsible for:

✔ Investigating misuse
✔ Taking disciplinary action
✔ Preventing leakages
✔ Recalling misused products

VCQRU only provides anti-fraud detection.

6.11 HANDLING FAKE PRODUCT OR DUPLICATE SCAN USERS

If a user reports:

- “Duplicate Code Detected”
- “Invalid Code”
- “Suspected Counterfeit”

Brand must:

✔ Investigate
✔ Validate purchase
✔ Provide customer support

✔ Decide replacement/refund
✔ Manage legal action

VCQRU only provides system-generated result.

6.12 USER REWARD BLOCKING DUE TO KYC FAILURE

If KYC is required for:

- High payouts
- TDS thresholds
- Compliance constraints

Brand must define:

✔ Rules to block reward
✔ Conditions to unblock
✔ Exceptions (if any)
✔ SMS/WhatsApp/email text for user communication

VCQRU does not decide exception handling.

6.13 BRAND FULL LIABILITY FOR USER ELIGIBILITY DISPUTES

If a user claims:

- "I am eligible for this scheme"
- "Why is cashback not given?"
- "Why is KYC rejected?"
- "Why was I blocked?"
- "Why are limits applied?"

Brand MUST respond.

VCQRU will only provide system logs, not decisions.

6.14 USER VERIFICATION AUDIT RESPONSIBILITY

Brand must:

✔ Conduct internal audits
✔ Verify correctness of approvals
✔ Check fraud patterns
✔ Ensure compliance with 194R
✔ Review suspicious users

VCQRU will NOT perform verification audits.

6.15 BRAND RESPONSIBILITY FOR USER PRIVACY CONSENT TEXT

Brand must provide:

✔ KYC consent text
✔ Data sharing consent
✔ PAN usage disclaimer
✔ Tax compliance consent
✔ Scheme rules consent
✔ Fraud penalty consent

VCQRU simply displays the text.

7.0 OVERVIEW

This section explains:

✔ What user data VCQRU collects

✔ How VCQRU protects it

✔ What the Brand is allowed / NOT allowed to do

✔ How consent works

✔ Who owns which privacy obligations

✔ How DPDP Act 2023 compliance is handled

✔ Indemnity rules for data misuse

This ensures **VCQRU stays legally safe** from ANY data misuse done by Brands.

7.1 TYPES OF USER DATA COLLECTED (Only What Is Required)

VCQRU collects only the minimum data required to operate:

Personal Identification Data

- Mobile number
- Name
- UPI ID
- PAN (only if brand requires)
- KYC documents (only if brand requires)

Behavioral Data

- Scans performed
- Device fingerprint
- IP address

- Location signals
- QR results

Transaction Data

- Points
- Cashback
- Rewards
- Payout history
- KYC status

Technical Data

- Browser info
- OS info
- Error logs
- OTP logs

VCQRU does **NOT** collect:

❌ Banking passwords
❌ ATM PIN
❌ CVV
❌ Aadhaar biometrics
❌ Sensitive financial credentials

7.2 DATA MINIMIZATION PRINCIPLE

VCQRU follows strict rules:

✔ Collect only what is necessary
✔ Store only for required period
✔ Delete data after legal retention time
✔ Never request excessive documents
✔ No hidden or forced data collection

This is fully aligned with **DPDP Act & GDPR principles**.

7.3 DATA STORAGE & ENCRYPTION

VCQRU ensures:

✔ **AES-256 encryption for stored data**

✔ **TLS 1.2+ encryption for transmitted data**

✔ **Encrypted PAN & UPI fields**

✔ **Access-controlled data vaults**

✔ **Separate production & staging environments**

✔ **Regular vulnerability audits**

✔ **Firewalled servers**

✔ **Daily backup & disaster recovery**

✔ **Activity monitoring & intrusion detection**

VCQRU guarantees **bank-level security**.

7.4 ROLE-BASED ACCESS CONTROL (RBAC)

Only authorized VCQRU employees can access user data:

✔ Access is role-based
✔ Need-to-know basis
✔ Logging of every access
✔ Regular access audits
✔ Mandatory confidentiality agreements
✔ Strict employee KYC & background verification

Brands NEVER get unrestricted access to user data.

7.5 BRAND ACCESS RESTRICTIONS (VERY IMPORTANT)

The Brand can ONLY access:

✔ User scan data
✔ Transaction data
✔ Redemption reports
✔ Program performance analytics
✔ KYC verification workflow (if required)

Brands cannot:

❌ Download entire user database
❌ Access raw data without permission
❌ Extract mobile numbers for marketing
❌ Sell user details
❌ Share user data with third parties
❌ Use data outside program scope

Brand must **formally commit**:

"User data will be used ONLY for program execution, not for marketing, sales, promotion, or resale."

This protects VCQRU from data misuse liability.

7.6 USER CONSENT POLICY

VCQRU ensures clear platform-level consent:

✔ Before login
✔ Before profile creation
✔ Before sharing PAN/KYC
✔ Before payout processing
✔ Before accessing location

Brand must provide its own Terms & Conditions, but **VCQRU handles consent workflow**.

7.7 DATA SHARING RULES (STRICT COMPLIANCE)

VCQRU shares data ONLY with:

✔ The Brand (program owner)
✔ Authorized payout partners (NPCI-integrated)
✔ Legal authorities (only under binding legal request)

VCQRU will NOT share data with:

❌ Third-party marketing companies
❌ Brand channel partners
❌ Distributors
❌ Retailers
❌ Sales agencies
❌ Any non-authorized entities

Brand must NEVER forward or share data with:

- Distributors
- Retailers
- Third-party marketing vendors
- Sales team (without written reason)
- External agencies

Brand is **fully liable** for any unauthorized sharing.

7.8 PURPOSE LIMITATION (DPDP Act Clause)

Data can be used ONLY for:

✔ Anti-counterfeit verification
✔ Loyalty & cashback programs
✔ Reward eligibility
✔ Fraud detection

✔ Program analytics
✔ Compliance (tax, audit, legal)

Data CANNOT be used for:

❌ Bulk marketing campaigns
❌ Cold calling
❌ WhatsApp broadcast promotions
❌ Social media targeting
❌ Customer reselling
❌ Any purpose outside program

Brand indemnifies VCQRU for misuse.

7.9 USER RIGHTS (Handled Through VCQRU)

Users may request:

✔ Data correction
✔ Data deletion
✔ Account closure
✔ Consent withdrawal
✔ KYC withdrawal
✔ Stop communication

Brand must honor these requests **when forwarded by VCQRU**.

7.10 DATA RETENTION & DELETION POLICY

VCQRU retains user data:

✔ For duration of the program
✔ For legally mandated compliance period
✔ For audit trails

After the retention period:

✔ Data is anonymized
or
✔ Securely deleted

Once deleted, **VCQRU cannot restore data**.

7.11 DATA BREACH RESPONSE PROCEDURE

VCQRU will:

✔ Investigate immediately
✔ Isolate affected systems

✔ Block unauthorized access
✔ Notify Brand within the required legal timeframe
✔ Provide incident report

Brand must:

✔ Notify impacted users (if required by law)
✔ Handle public communication (if needed)
✔ Cooperate with legal authorities

VCQRU provides technical support only.

7.12 BRAND LIABILITY FOR MISUSE OF DATA

Brand agrees:

Any misuse, unauthorized sharing, or illegal usage of user data is 100% Brand responsibility.

Brand must indemnify VCQRU against:

✔ Complaints
✔ Legal notices
✔ DPDP investigations
✔ Penalties
✔ Lawsuits
✔ Regulatory action

VCQRU is protected completely.

7.13 COMPLIANCE WITH DPDP ACT & IT ACT

Brand must:

✔ Follow DPDP Act 2023
✔ Follow IT Act 2000
✔ Follow RBI/NPCI data rules
✔ Appoint a compliance officer (if required)

VCQRU ensures platform-level compliance only.

8.0 OVERVIEW

This section defines:

- What fraud VCQRU can detect
- How fraud detection works
- What is Brand responsibility
- What VCQRU is *not* liable for
- Who takes action

- Who bears losses
- What VCQRU flags automatically

VCQRU provides the **technology**, but:

All fraud-related financial, legal & operational responsibility lies on the Brand.

8.1 TYPES OF FRAUD VCQRU CAN DETECT (TECHNICAL DETECTION ONLY)

VCQRU automatically identifies suspicious patterns such as:

✔ **Product-related:**

- Duplicate QR scans
- Invalid or unregistered codes
- Counterfeit label patterns
- Rapid multiple scans of same code
- Product not associated with SKU/batch

✔ **User-related:**

- Multi-account abuse
- Same user using multiple numbers
- Same device for multiple accounts
- Shared UPI IDs across users
- Shared PAN across multiple accounts

✔ **Location-related:**

- GPS spoofing
- VPN usage
- Unusual location jumps
- Scan outside permitted region

✔ **Device-related:**

- Rooted or jailbroken device
- Emulators
- Browser manipulation
- Auto-click scripts

8.2 VCQRU'S ROLE IN FRAUD DETECTION

VCQRU provides the following **technical & automated** functions:

✔ Detection
✔ Logging
✔ Alerts on dashboard
✔ Fraud score indicators

✔ Blocking signals (if configured)
✔ Reports for brand review

VCQRU does NOT:

❌ Investigate fraud
❌ Decide user guilt
❌ Block a user without brand approval
❌ Penalize users
❌ Reverse points/cashback
❌ Take legal action
❌ Handle retailer/distributor fraud cases

These decisions belong to the **Brand ONLY**.

8.3 BRAND RESPONSIBILITY FOR INVESTIGATION & ACTION

Brand must:

✔ Investigate flagged cases
✔ Call/verify user if required
✔ Review suspicious patterns
✔ Decide whether to block user
✔ Decide whether to reverse rewards
✔ Handle complaints & appeals
✔ Take legal action against fraudsters
✔ Investigate supply chain misuse
✔ Validate counterfeit incidents
✔ Ensure genuine users are rewarded correctly

VCQRU is not liable for delays or wrong decisions taken by the Brand.

8.4 SUPPLY CHAIN FRAUD (DISTRIBUTORS/RETAILERS/DEALERS)

Supply chain misuse includes:

- Codes leaked by distributors
- Retailers scanning codes before selling
- Warehouse team misusing codes
- Middlemen reselling unused labels
- Bulk scanning before field release

Brand is responsible for:

✔ Supply chain integrity
✔ Monitoring distributor activity
✔ Investigating retailer misuse
✔ Removing fraudulent channel partners
✔ Ensuring secure packaging & QC

VCQRU provides only **technical evidence**, not legal handling.

8.5 COUNTERFEIT PRODUCT HANDLING (BRAND ONLY)

If a user receives:

- "Invalid Code"
- "Duplicate Code Detected"
- "Suspected Counterfeit"

Brand must:

✔ Investigate product source
✔ Request purchase proof (if needed)
✔ Decide refund/replacement
✔ Take legal action against counterfeiters
✔ Inform law enforcement (if required)

VCQRU does NOT:

❌ Validate physical product
❌ Handle consumer refund
❌ Replace product
❌ File FIR or legal case
❌ Participate in investigations

Brand is fully responsible.

8.6 INTERNAL TEAM OR AGENCY FRAUD (BRAND LIABILITY)

Fraud can also originate from:

- Brand sales team
- Brand field executives
- Market agencies
- Packaging vendors
- Distributors misusing the system

Brand must:

✔ Investigate internally
✔ Take disciplinary action
✔ Review audit logs
✔ Protect integrity of the program

VCQRU provides logs only, not investigation.

8.7 FRAUD IMPACT ON PAYOUTS (BRAND LIABILITY)

Brand bears full responsibility for losses due to:

- Fraud users
- Fake KYCs
- Duplicate scans
- Dealer misuse
- Blacklisted users bypassing rules
- Wrong rewards given due to brand error

VCQRU carries **zero liability**.

8.8 ANTI-FRAUD SYSTEM FEATURES PROVIDED BY VCQRU

VCQRU provides:

✔ Real-time fraud alerts
✔ Device fingerprinting
✔ User behaviour tracking
✔ High-frequency scan flags
✔ Repeat code flags
✔ Batch-level fraud patterns
✔ Location mismatch alerts
✔ IP address anomaly detection
✔ KYC/PAN duplication alerts
✔ Usage heatmaps
✔ Suspicious redemption patterns

Brand receives **data & signals** only.

8.9 BRAND MUST TAKE DECISIONS ON FRAUD

Brand decides:

✔ Blacklist
✔ Block
✔ Reject KYC
✔ Freeze wallet
✔ Reverse points
✔ Withhold cashback
✔ Demand more documents
✔ Delete user account
✔ Take police/legal action

VCQRU implements actions *only* after Brand approval.

8.10 WRONG OR DELAYED BRAND ACTIONS — BRAND LIABILITY

If Brand:

- delays action
- ignores fraud
- mishandles user disputes
- allows fraudulent payouts
- wrongly blocks a genuine user

VCQRU is NOT liable for:

❌ financial loss
❌ brand reputation damage
❌ legal disputes
❌ consumer complaints
❌ tax leakage
❌ misuse of system

8.11 SCHEME MISUSE BY WRONG AUDIENCE

If:

- A dealer pretends to be mechanic
- A retailer pretends to be consumer
- Same user uses multiple numbers
- Same UPI used across multiple accounts
- Household misuse happens
- Agency employees misuse codes

BRAND must handle:

✔ Eligibility enforcement
✔ Manual verification
✔ Blacklisting
✔ Reversals

VCQRU only detects patterns.

8.12 LEGAL INDEMNIFICATION FOR FRAUD

Brand indemnifies VCQRU against ANY fraud-related:

✔ Legal claims
✔ Monetary losses
✔ User complaints
✔ Government notices
✔ Investigations
✔ Chargebacks
✔ Penalties

This clause fully protects VCQRU.

8.13 LIMITATION OF LIABILITY FOR FRAUD LOSSES

VCQRU shall NOT be held responsible for:

❌ Fraud caused by wrong rules
❌ Fraud caused by brand miscommunication
❌ Fraud caused by supply chain misuse
❌ Counterfeit product proliferation
❌ Wrong approvals of KYC
❌ Incorrect user eligibility
❌ Budget loss due to program misuse

Brand carries all losses.

9.0 OVERVIEW

This section defines:

- Who manages customer support
- Who resolves user complaints
- Who handles reward/payout disputes
- Who handles product issues
- Brand vs VCQRU responsibilities
- Legal obligations
- Communication channels
- Escalation rules

When a user raises a complaint, **BRAND is the primary owner** of resolution.

VCQRU only provides **technical platform support**, not program support.

9.1 BRAND IS THE PRIMARY OWNER OF ALL USER SUPPORT

The Brand must provide:

✔ Customer care team
✔ Email support
✔ WhatsApp support (if chosen)
✔ Toll-free number (if required)
✔ Field/Dealer support team
✔ Complaint tracking system
✔ Response timelines (internal SLA)
✔ Scheme rule clarifications

VCQRU supports ONLY:

✔ OTP issues
✔ Scan failure (technical)
✔ Login issues

✔ Platform downtime
✔ Browser/app issues

NOT program-related issues.

9.2 TYPES OF COMPLAINTS BRAND MUST HANDLE DIRECTLY

The Brand must handle ALL non-technical issues such as:

Reward & Points Issues

- “My points are not correct”
- “Why did my points reduce?”
- “Points not credited after scan”
- “Points expired”
- “Wrong points given”

Cashback Issues

- “I did not receive cashback”
- “Cashback sent to wrong UPI”
- “Delay in crediting cashback”
- “Less cashback credited”

Tax (TDS) Related Issues

- “Why is TDS deducted?”
- “Where is my Form 16A?”
- “PAN mismatch in TDS”

KYC Issues

- “Why is my KYC rejected?”
- “Why do you need PAN?”
- “KYC pending for long time”

Eligibility Issues

- “I am a mechanic, why not eligible?”
- “Why is my category wrong?”

Product-Related Complaints

- “This product is fake”
- “Duplicate scan message received”
- “Product damaged”
- “Retailer gave me wrong product”

Scheme Rules & Benefits

- “What is the reward?”
- “Why is my reward not approved?”
- “Why is redemption blocked?”

VCQRU DOES NOT handle any of the above issues.

9.3 VCQRU RESPONSIBILITIES (TECH SUPPORT ONLY)

VCQRU will ONLY handle:

✔ Platform technical issues
✔ Server uptime
✔ Scan engine issues
✔ OTP not received
✔ Login issues
✔ App/page loading issues
✔ Payout API technical error (logs only)
✔ Dashboard access issues
✔ Data mismatches due to technical bugs

VCQRU WILL NOT:

❌ Approve/Reject KYC
❌ Approve/Reject payouts
❌ Handle reward eligibility
❌ Explain brand scheme rules
❌ Speak to end-users
❌ Resolve counterfeit disputes
❌ Manage user personal issues
❌ Interact with channel partners

9.4 BRAND MUST PROVIDE USER COMMUNICATION TEMPLATES

Brand must provide all the user-facing content:

✔ SMS templates
✔ WhatsApp templates
✔ In-app notifications
✔ FAQs
✔ Help center content
✔ Customer care numbers
✔ Program rules
✔ Terms & conditions
✔ Appeal process

VCQRU will not write or finalize program terms.

9.5 ESCALATION MATRIX (Brand Must Create)

Brand must define multi-level support:

Level 1 – Customer Care

Handles: Basic user complaints

Level 2 – Brand Program Team

Handles: Reward, eligibility, KYC issues

Level 3 – Brand Finance Team

Handles: Payout disputes, tax issues

Level 4 – Brand Legal Team

Handles: Counterfeit, legal claims

VCQRU is NOT part of escalation unless technical logs are needed.

9.6 HANDLING DISPUTES ABOUT WRONG REWARD OR WRONG BENEFIT

If user complains:

- “I should have received ₹10, but I got ₹5”
- “Reward calculation is wrong”
- “Why is my claim rejected?”

Brand must:

✔ Review dispute
✔ Check brand rules
✔ Decide final reward
✔ Communicate decision to user

VCQRU only provides:

✔ Scan logs
✔ Rule execution logs
✔ Transaction history

VCQRU does NOT make decisions.

9.7 HANDLING PRODUCT AUTHENTICITY DISPUTES

If user complains the product is:

- Fake
- Duplicate
- Tampered

- Refurbished

Brand must:

✔ Investigate product
✔ Validate purchase proof
✔ Replace/refund (if needed)
✔ Handle legal & consumer cases
✔ File FIR (if required)

VCQRU only provides:

✔ Scan authenticity result
✔ Label-level data

NO product involvement.

9.8 HANDLING PAYMENT/PAYOUT DISPUTES

If payout fails due to:

- Wrong UPI
- Bank downtime
- Server error
- Limit breach
- Reversal
- TDS deduction

Brand must:

✔ Handle dispute
✔ Reprocess if needed
✔ Bear financial responsibility

VCQRU provides:

✔ Logs
✔ API response
✔ Error codes

But does NOT resolve financial disputes.

9.9 HANDLING SCHEME MISCOMMUNICATION

If user claims:

- “I was told this reward is ₹50”
- “Retailer said something else”
- “Your sales team promised more points”
- “Dealer told wrong information”

Brand must:

✔ Correct communication
✔ Handle user objection
✔ Clarify rules

VCQRU is not responsible for brand miscommunication.

9.10 HANDLING SOCIAL MEDIA NEGATIVE COMMENTS

If users post:

- On Facebook
- Instagram
- Twitter
- WhatsApp
- Play Store
- YouTube

Brand must:

✔ Monitor comments
✔ Respond professionally
✔ Resolve user issues
✔ Manage reputation risk

VCQRU is NOT responsible for:

❌ Public complaints
❌ Image damage
❌ Social media replies
❌ Reputation management

9.11 BRAND MUST MAINTAIN SUPPORT LOGS

Brand must:

✔ Maintain complaint logs
✔ Record resolutions
✔ Track SLAs
✔ Provide audit reports

VCQRU provides technical logs only.

9.12 FINAL USER DISPUTE RESPONSIBILITY (BRAND ONLY)

Brand is 100% responsible for:

✔ User happiness
✔ Resolving rewards issues
✔ Handling payment disputes
✔ Managing miscommunication
✔ Handling product disputes
✔ Addressing legal demands
✔ Filing responses to authorities

VCQRU is fully indemnified.

10.0 OVERVIEW

This section governs the responsibilities of the **Brand** and **VCQRU** related to:

✔ Product authenticity
✔ Batch & SKU mapping
✔ Label/QR generation
✔ Counterfeit detection
✔ Consumer complaints regarding fake products
✔ Market-level misuse
✔ Wrong uploads of label data
✔ Legal responsibility in counterfeit cases

The objective is to ensure **VCQRU remains 100% safe** from product-level liabilities.

10.1 BRAND IS THE SOLE OWNER OF PRODUCT AUTHENTICITY

Brand acknowledges that:

VCQRU does NOT manufacture, package, or distribute the product.

VCQRU does NOT guarantee physical product authenticity.

VCQRU system ONLY verifies codes mapped by the Brand.

Therefore, the Brand is fully responsible for:

✔ Real product quality
✔ Genuine items in the market
✔ Consumer complaints
✔ Legal & safety compliance
✔ Market recalls
✔ Warranty handling
✔ Counterfeit incidents

VCQRU has no involvement in product manufacture or physical inspection.

10.2 BRAND RESPONSIBILITY FOR LABEL/QR/HOLOGRAM DATA

Brand must:

✔ Upload correct SKU data
✔ Upload correct batch numbers
✔ Upload correct label series
✔ Map QR codes to correct SKU
✔ Ensure no duplicate label range
✔ Ensure printer follows correct procedure
✔ Validate label sample before market launch
✔ Prevent unauthorized printing

VCQRU simply hosts and validates the data provided.

VCQRU IS NOT RESPONSIBLE FOR:

- Incorrect label uploads
- Wrong SKU/batch mapping
- Misprints by printing vendor
- Wrong artwork shared by brand
- Label duplication by unauthorized parties

All errors are BRAND responsibility.

10.3 BRAND RESPONSIBILITY TO ENSURE LABEL SECURITY

Brand must:

✔ Use authorized printing partners
✔ Ensure secure transportation of labels
✔ Track label distribution (warehouse → distributor)
✔ Prevent stolen/misused label stocks
✔ Audit packaging vendors
✔ Maintain strict QC processes
✔ Prevent internal leakage

VCQRU is NOT responsible for label theft or supply chain misuse.

10.4 VCQRU'S ROLE IN AUTHENTICATION (TECHNOLOGY ONLY)

VCQRU provides:

✔ QR code verification engine
✔ Duplicate scan alerts
✔ First-scan validation
✔ Batch, expiry & MRP mapping
✔ Fraud detection signals
✔ Counterfeit analytics dashboard
✔ Geo-tagging of suspicious scans

VCQRU does NOT:

❌ Inspect the physical product
❌ Confirm product safety
❌ Confirm expiry correctness
❌ Examine packaging quality
❌ Validate label printing accuracy
❌ Validate hologram printing quality

VCQRU only shows RESULTS based on brand-provided data.

10.5 BRAND RESPONSIBILITY FOR COUNTERFEIT CASES

If counterfeit products appear in the market, Brand must:

✔ Investigate source
✔ Trace supply chain leak
✔ Validate product samples
✔ File legal complaints
✔ Take consumer safety actions
✔ Manage recall (if needed)
✔ Update VCQRU with new batches or corrections
✔ Handle all PR and customer sentiment

VCQRU does NOT take part in:

❌ Market raids
❌ FIR filing
❌ Field investigations
❌ Product collection & testing
❌ Customer compensation
❌ Legal enforcement

10.6 BRAND RESPONSIBILITY FOR FAKE PRODUCT USER COMPLAINTS

If a user reports:

- “Invalid code”
- “Duplicate code”
- “Fake product suspected”
- “Tampered product”

Brand must:

✔ Directly communicate with user
✔ Ask for purchase proof (if needed)
✔ Request product photos
✔ Conduct quality inspection
✔ Provide refund/replacement

✔ Issue safety notices
✔ Take legal action against source

VCQRU ONLY shows scan result logs.

10.7 BRAND MUST NOT MISUSE AC ENGINE DATA FOR PUNISHING USERS

If user receives “Duplicate Scan”:

Brand must verify:

✔ Whether dealer/retailer misused code
✔ Whether product was scanned earlier
✔ Whether supply chain leaked codes
✔ Whether genuine user got wrong label

VCQRU recommends:

✔ Investigate
✔ Confirm
✔ THEN take action

Brand is responsible for wrong punitive action.

10.8 BRAND IS RESPONSIBLE FOR MISCONFIGURATION OF AUTHENTICITY RULES

If Brand:

- Uploads wrong label series
- Uploads wrong batch mapping
- Assigns duplicate codes
- Uploads expired product as active
- Releases wrong SKU with incorrect mapping
- Incorrectly configures traceability rules

VCQRU is NOT responsible for:

❌ Wrong “Fake Product” alerts
❌ Wrong “Duplicate Scan” messages
❌ Wrong “Authentic Product” results
❌ Loss of brand reputation
❌ Customer anger
❌ Supply-chain confusion

Brand owns 100% responsibility.

10.9 LOCATION-BASED AUTHENTICATION LOGIC

If brand defines:

✔ Region-specific SKUs
✔ State-blocked SKUs
✔ Export-only product
✔ Dealer-specific product flow

Brand must:

✔ Upload correct geolocation logic
✔ Ensure dealer compliance
✔ Track misuse

VCQRU only enforces logic as given.

10.10 BRAND MUST UPDATE VCQRU BEFORE CHANGING PACKAGING / LABEL DESIGN

If brand makes ANY change:

✔ Label size
✔ QR placement
✔ Artwork alignment
✔ Printing pattern
✔ Batch coding format
✔ New SKU launch
✔ Discontinuation of SKU

Brand MUST inform VCQRU before product reaches market.

If not, users may get incorrect scan results.

VCQRU is not liable if:

❌ Brand releases new packaging without informing
❌ Wrong scan results appear
❌ QR code unreadable
❌ Users complain

10.11 HANDLING OF MARKET SCAN SPIKES (FRAUD / COUNTERFEIT)

VCQRU detects:

✔ Abnormal clusters of scans
✔ Unusual location behavior
✔ First-scan surge in specific region
✔ Device-level fraud
✔ Rack-level misuse
✔ Counterfeit printing patterns

Brand must:

✔ Investigate on ground
✔ Find source of counterfeit
✔ Take legal action
✔ Issue press or retailer notices

VCQRU cannot act on-ground.

10.12 BRAND LEGAL LIABILITY FOR PRODUCT SAFETY & AUTHENTICITY

Brand acknowledges:

VCQRU cannot be held responsible for product harm, safety issues, counterfeit losses, legal claims, or consumer damages.

Brand indemnifies VCQRU against:

✔ Product failure claims
✔ Fake product health issues
✔ Dealer misuse
✔ Distributor negligence
✔ Wrong scan results due to incorrect data
✔ Compensation claims
✔ Consumer court cases
✔ Regulatory actions

10.13 LIABILITY EXCLUSION FOR VCQRU

VCQRU will NOT be liable for:

❌ Product quality
❌ Wrong label printing
❌ Wrong QR placement
❌ Data errors by brand
❌ Fake product circulation
❌ Supply chain tampering
❌ Wrong SKU mapping
❌ Expired product issues
❌ Market disruption

Brand bears ALL risks.

11.0 OVERVIEW

This section defines:

✔ How program changes must be handled
✔ How rules are implemented
✔ What approvals are required

✔ What happens if brand changes rules mid-way
✔ What VCQRU is responsible for
✔ What the brand MUST take responsibility for
✔ User communication obligations
✔ Suspension or termination of schemes

This ensures the program runs smoothly with **clear accountability**.

11.1 BRAND RESPONSIBILITY FOR PROGRAM LAUNCH READINESS

Before any program goes LIVE, the brand must:

✔ Approve the final rules
✔ Approve the SKU/batch mapping
✔ Approve user eligibility logic
✔ Approve cashback/points slabs
✔ Approve fraud logic
✔ Approve communication templates
✔ Approve program SOP
✔ Test and validate flows
✔ Complete funding of wallets
✔ Confirm tax (TDS) logic

VCQRU will **not** roll out the program unless brand approval is documented.

11.2 VCQRU EXECUTES ONLY WHAT BRAND APPROVES

VCQRU's responsibility:

✔ Implement the logic EXACTLY as approved
✔ Test the build (UAT)
✔ Deploy to production
✔ Ensure platform availability
✔ Provide logs & dashboards

VCQRU does NOT:

❌ Decide rules
❌ Define rewards
❌ Modify logic on its own
❌ Judge eligibility
❌ Change payouts

The brand *fully owns* the rules.

11.3 BRAND MUST PROVIDE ALL FINAL CONTENT

Brand is responsible for:

✔ Rule document
✔ Terms & conditions
✔ User-facing content
✔ Scheme benefits text
✔ KYC requirements
✔ Reward tables
✔ Points/cashback slabs
✔ Eligibility descriptions
✔ Validity
✔ Disclaimers
✔ Penalty rules

VCQRU only uploads content — not create or validate it.

11.4 MID-PROGRAM RULE CHANGE POLICY

Brands frequently request:

- Change of slabs
- Change of cashback amount
- New eligibility criteria
- New KYC requirements
- New roles or user types
- Different product mapping
- Scheme extensions
- Scheme expiry
- Points expiry adjustment
- Blacklist rule changes

All of these must follow strict rules.

Every change must be:

✔ Documented
✔ Submitted officially
✔ Approved by authorized brand signatory
✔ Undergo impact analysis
✔ Undergo technical/QA testing
✔ Communicated to VCQRU in writing
✔ Communicated to all users by the Brand

VCQRU only executes after formal approval.

11.5 BRAND RESPONSIBILITY FOR CHANGE IMPACT

If a brand changes rules mid-way, it must handle:

✔ User dissatisfaction
✔ Negative feedback

✔ Complaint escalation
✔ Financial impact
✔ Legal responsibility
✔ TDS recalculation (if applicable)
✔ Reward mismatch issues
✔ KYC requirement changes

VCQRU is fully protected because:

❗ **All consequences of rule changes = BRAND LIABILITY ONLY.**

11.6 BRAND MUST COMMUNICATE ALL CHANGES TO USERS

If brand changes:

- Slabs
- Cashback
- Points
- Expiry
- Eligibility
- KYC
- Rewards
- Product lists

Brand MUST:

✔ Notify users
✔ Update website/WhatsApp communications
✔ Update product packaging (if required)
✔ Inform channel partners
✔ Update dealers/retailers

VCQRU does NOT communicate changes to users.

11.7 EMERGENCY CHANGES (Fraud or Legal Requirement)

If:

- Large-scale fraud is detected
- Legal restriction is applied
- Government mandates change
- Counterfeit cases spike
- Product recall is initiated

Brand MUST:

✔ Provide immediate instructions
✔ Approve urgent configurations

✔ Handle legal/regulatory communication
✔ Manage user-facing messaging

VCQRU will only update technical configurations.

11.8 PROGRAM PAUSE, HOLD OR TERMINATION

If the Brand pauses or terminates a program:

Brand must:

✔ Clear all pending payouts
✔ Inform all users
✔ Stop promotions & advertising
✔ Manage user disappointment
✔ Handle legal responsibility
✔ Handle supply chain changes
✔ Manage market expectations

VCQRU will:

✔ Disable authentication/rewards as instructed
✔ Archive data
✔ Provide reports

VCQRU is NOT responsible for:

❌ User complaints
❌ Pending benefits
❌ Market confusion
❌ Field/sales team miscommunication

11.9 VERSION CONTROL & DOCUMENT MANAGEMENT

Brand must maintain:

✔ Latest version of program rules
✔ Change logs
✔ Program revision history
✔ Approval trail for every update
✔ Date/time of rule changes

VCQRU will maintain internal logs of:

✔ Technical changes
✔ System configurations
✔ Deployment timestamps

11.10 MISCOMMUNICATION OR FALSE PROMISES BY BRAND SALES TEAM

If Brand's sales or marketing teams promise users:

- Higher rewards
- Wrong cashback amounts
- Incorrect slabs
- Benefits not included in program
- Unofficial discounts

Brand bears FULL responsibility.

VCQRU is not accountable for:

❌ Miscommitments
❌ Dealer-level incentives
❌ Sales team errors
❌ Verbal promises

11.11 UNAPPROVED CAMPAIGNS OR PROMOTIONS

If the Brand's field or marketing teams run:

✔ WhatsApp promotions
✔ Social media contests
✔ Flyers with wrong info
✔ Dealer promotions

…that do not match the approved scheme:

Brand must:

✔ Correct the communication
✔ Handle user complaints
✔ Provide compensations (if any)

VCQRU will ONLY follow approved logic.

11.12 BRAND LIABILITY FOR ALL PROGRAM EXECUTION FAILURES

The Brand is legally responsible for:

✔ Wrong or incomplete rules
✔ Poor forecasting
✔ Over-redemption
✔ User dissatisfaction
✔ Illegal scheme structure
✔ Invalid promotions
✔ Sales/marketing errors
✔ KYC mismanagement

✔ TDS miscalculation
✔ Budget shortages
✔ Reward miscommitments

VCQRU is indemnified against ANY such issues.

12.0 OVERVIEW

This section defines:

✔ How the Brand must manage payout reconciliation
✔ What VCQRU provides as evidence
✔ Who is responsible for mismatches
✔ How disputes must be resolved
✔ How financial summaries must be reviewed
✔ What happens at program closure
✔ What settlement rules apply

VCQRU's role is **technical**, while the Brand owns the **financial responsibility**.

12.1 BRAND RESPONSIBILITY FOR DAILY RECONCILIATION

The Brand MUST perform daily reconciliation of:

✔ Scans vs. rewards
✔ Points issued vs. points redeemed
✔ Cashback issued vs. wallet balance
✔ KYC approved vs. KYC pending
✔ Successful UPI payouts
✔ Failed UPI payouts
✔ Reversed payouts
✔ Duplicate payouts
✔ Disputed transactions
✔ TDS deductions (if applicable)

VCQRU only provides:

✔ Logs
✔ Reports
✔ API response history
✔ Admin dashboard analytics

Brand must review and validate.

12.2 WEEKLY RECONCILIATION (MANDATORY FOR ALL BRANDS)

At least once every week, Brand must:

✔ Compare wallet balance vs. program cost
✔ Check outstanding payouts
✔ Review suspicious transactions
✔ Review user-level payouts over threshold
✔ Validate KYC-triggered payouts
✔ Reconcile GST/TDS if applicable
✔ Identify fraud patterns

VCQRU acts as data provider — NOT validator.

12.3 MONTHLY RECONCILIATION & SIGN-OFF

Every month, the Brand must:

✔ Validate all cashbacks
✔ Validate total rewards
✔ Validate total payouts
✔ Validate TDS deductions
✔ Validate total scans
✔ Validate total user acquisition
✔ Validate program ROI

Brand must sign:

✔ Monthly Settlement Summary
✔ Monthly Reward Ledger
✔ Monthly TDS Summary

VCQRU only provides exportable data.

12.4 VCQRU IS NOT RESPONSIBLE FOR RECONCILIATION FAILURE

If Brand forgets to reconcile and later finds:

❌ Duplicate payouts
❌ Extra rewards
❌ Wrong points
❌ Over-redemption
❌ KYC fraud
❌ Dealer/retailer misuse
❌ Budget shortage
❌ TDS mismatch

VCQRU holds **zero liability**.

Brand must absorb the financial impact.

12.5 BRAND RESPONSIBILITY FOR DISPUTE RESOLUTION

Any dispute raised by:

- Users
- Channel partners
- Retailers
- Distributors
- Government authorities
- Banks/NPCI
- Sales teams

Brand must:

✔ Investigate
✔ Validate logs
✔ Reconcile amounts
✔ Make corrective payouts
✔ Issue refunds (if needed)
✔ Handle user complaints

VCQRU only shares logs; it does NOT resolve disputes.

12.6 RESPONSIBILITY FOR FAILED OR PENDING PAYOUTS (BRAND ONLY)

If payout fails due to:

- Wrong UPI
- Bank issue
- Daily UPI limit crossed
- Server downtime
- Insufficient brand wallet balance
- KYC mismatch
- TDS deduction error

Brand must:

✔ Investigate
✔ Reprocess (if needed)
✔ Pay pending amount
✔ Bear losses
✔ Update users

VCQRU hosts logs, not funds.

12.7 UPI/NEFT TRANSACTION RECONCILIATION

Brand must:

✔ Match VCQRU logs with payout partner logs
✔ Compare success/failure codes
✔ Verify settlement statements

✔ Reconcile bank/NPCI settlements
✔ Manage reversals manually if needed

VCQRU will NEVER:

❌ Manage bank accounts
❌ Handle settlement discrepancies
❌ Liaise with banks on behalf of Brand

12.8 RECONCILIATION OF TAX (TDS 194R)

Brand must reconcile:

✔ PAN-based reward payouts
✔ Total TDS deducted
✔ TDS challan payments
✔ Statement of 26Q returns
✔ Form 16A issuance
✔ TDS mismatches
✔ Higher TDS cases (no PAN)

VCQRU only provides data extraction.

12.9 FINANCIAL REPORTS PROVIDED BY VCQRU

VCQRU provides:

✔ User-wise reward summary
✔ Transaction report
✔ Program summary report
✔ Scan report
✔ Fraud alert report
✔ KYC summary
✔ Payout logs (success/failure)
✔ Reversal logs
✔ Scheme performance dashboards

Brand must analyze all reports regularly.

12.10 PROGRAM-LEVEL FINANCIAL CLOSURE

When the program ends, Brand must:

✔ Clear all pending payouts
✔ Approve final ledger
✔ Approve last reconciliation report
✔ Clear remaining funds
✔ Provide TDS compliance proofs

✔ Verify fraud cases
✔ Approve closure certificate

VCQRU closes technical access ONLY after brand confirmation.

12.11 BRAND MUST CLEAR ALL DUES BEFORE TERMINATION

Before the Brand exits or pauses a program:

Brand must:

✔ Clear pending amounts
✔ Clear pending UPI payouts
✔ Clear pending point redemptions
✔ Clear pending KYC-linked payouts
✔ Clear tax liabilities
✔ Clear system usage fees
✔ Clear outstanding invoices

VCQRU will NOT be responsible for unsettled liabilities.

12.12 BRAND LIABILITY FOR FINANCIAL MISMATCHES

Brand agrees that:

🟥 **All mismatches → Brand liability**

🟥 **All payout errors → Brand liability**

🟥 **All reconciliation delays → Brand liability**

🟥 **All budget gaps → Brand liability**

🟥 **All duplicate payouts → Brand liability**

🟥 **All fake KYC rewards → Brand liability**

🟥 **All TDS differences → Brand liability**

VCQRU is only a data provider.

12.13 INDEMNITY AGAINST FINANCIAL LOSS

Brand shall indemnify, defend & hold harmless VCQRU against ALL financial losses arising from:

✔ Wrong payouts
✔ Unauthorized payouts
✔ Brand-side fraud

✔ Incorrect reward rules
✔ User eligibility error
✔ Wrong KYC approvals
✔ Program mismanagement
✔ TDS non-compliance
✔ Government audits

This clause gives VCQRU COMPLETE LEGAL PROTECTION.

13.0 OVERVIEW

This section defines:

✔ Who is legally responsible (Brand vs VCQRU)
✔ What legal compliance the Brand must follow
✔ What regulations apply
✔ How indemnity works
✔ What VCQRU is NOT liable for
✔ Limitation of liability
✔ Disclaimers
✔ Governing law & dispute resolution

13.1 BRAND'S FULL REGULATORY COMPLIANCE RESPONSIBILITY

Brand must comply with ALL laws applicable to:

✔ Manufacturing

✔ Product safety

✔ Labeling & packaging

✔ Consumer protection

✔ Anti-counterfeit compliance

✔ Channel partner schemes

✔ Cashback schemes

✔ Loyalty programs

✔ Data privacy (DPDP)

✔ Advertising & promotional rules

✔ TDS (Section 194R)

✔ **AML & KYC norms**

✔ **GST (if applicable)**

✔ **NPCI/RBI guidelines for UPI payouts**

VCQRU is **only** a technology provider — not a regulatory entity.

13.2 BRAND RESPONSIBILITY FOR PROGRAM LEGALITY

Brand confirms that:

✔ All schemes launched are legally valid
✔ Rewards issued follow all regulations
✔ Program does not violate competition laws
✔ Program does not mislead customers
✔ Program follows Consumer Protection Act
✔ Program is approved internally by the Brand
✔ Brand is legally empowered to run such schemes

VCQRU has **no obligation** to verify legality of Brand programs.

13.3 BRAND MUST ENSURE COMPLIANCE WITH CONSUMER PROTECTION LAWS

Brand must ensure:

✔ All communication is correct & honest
✔ No false or misleading claims are made
✔ Product authenticity claims follow rules
✔ All public promises are fulfilled
✔ All dispute resolutions follow legal timelines

If any user files a legal case:

➡ Brand is fully responsible
➡ VCQRU is NOT to be made a party

13.4 INDEMNITY CLAUSE (VERY IMPORTANT)

The Brand agrees to indemnify, defend, and hold harmless VCQRU against ALL claims, costs, liabilities, losses, damages, penalties, suits, litigation, government notices, and expensesarising out of:

✔ Product authenticity issues
✔ Fake/duplicate product disputes
✔ Counterfeit claims
✔ Wrong payout or reward
✔ Tax disputes (TDS/GST/Income Tax)

✔ Wrong KYC approvals
✔ User eligibility disputes
✔ Breach of program rules
✔ Miscommunication by Brand
✔ Data misuse by Brand
✔ Distributor/retailer abuse
✔ Supply chain fraud
✔ Compliance lapses
✔ Program failure or shutdown
✔ Budget shortages
✔ Any legal notice from consumer

Indemnity includes legal fees, damages, settlement costs, government penalties, and compensation claims.

VCQRU is fully protected.

13.5 VCQRU IS NOT LIABLE FOR ANY BRAND-SIDE MISCONDUCT

VCQRU is NOT responsible for:

❌ Misleading marketing by the Brand
❌ Wrong promises made by sales teams
❌ Incorrect scheme details communicated by distributors
❌ Wrong rewards or payouts
❌ Misprinted packaging
❌ Misconfigured eligibility rules
❌ Unapproved promotional claims
❌ Misuse of system by retail partners
❌ Dealership-level misuse
❌ Field-force fraud

Brand bears 100% responsibility.

13.6 VCQRU IS NOT LIABLE FOR ANY USER CLAIMS

If a user files a complaint about:

- Fake product
- Wrong payout
- Missing cashback
- Wrong points
- KYC rejection
- Wrong detection of authenticity
- Product safety issue
- Warranty claim
- Physical injury from product
- Expired/defective product

- Miscommunication
- Scheme confusion

Brand MUST handle 100% of such cases.

VCQRU will provide only system logs.

13.7 LIMITATION OF LIABILITY (EXTREMELY IMPORTANT)

VCQRU's maximum liability is:

Limited to the value of 1 month of platform fees paid by the Brand.

VCQRU is NOT liable for:

❌ Loss of business
❌ Loss of profit
❌ Loss of brand reputation
❌ Legal penalties
❌ Consequential damages
❌ Punitive damages
❌ Government fines
❌ Indirect losses
❌ Fraud losses
❌ Operational delays
❌ Supply chain issues

This protects VCQRU from unlimited liability.

13.8 DISCLAIMERS

VCQRU disclaims responsibility for:

✔ Accuracy of brand data
✔ Product authenticity
✔ Scheme structure
✔ Program communication
✔ Marketing claims
✔ Financial correctness
✔ User disputes
✔ Manufacturing or packaging issues
✔ Incorrect brand rules

VCQRU provides “as is” and “as configured by Brand” execution.

13.9 FORCE MAJEURE CLAUSE

VCQRU is NOT responsible for delays due to:

✔ Natural disasters
✔ Government restrictions
✔ Telecom outages
✔ Server downtime from cloud providers
✔ Cyber-attacks from third parties
✔ War/riots/strikes
✔ Pandemic restrictions

Brand must accept all consequences.

13.10 GOVERNING LAW & JURISDICTION

This agreement follows:

✔ Indian Contract Act
✔ Information Technology Act 2000
✔ DPDP Act 2023
✔ Income Tax Act (194R, etc.)
✔ NPCI/RBI payout rules

Jurisdiction:

All disputes will be handled ONLY in courts of Gurugram, Haryana, India.

Brand agrees not to file legal cases elsewhere.

13.11 DISPUTE RESOLUTION (MANDATORY)

Before legal escalation:

1. Internal escalation
2. Senior management discussion
3. Mediation (if needed)
4. Arbitration under the Arbitration & Conciliation Act

VCQRU cannot be forced into lengthy litigation unless arbitration fails.

13.12 COMPLIANCE AUDITS (BRAND RESPONSIBILITY)

Brand agrees to:

✔ Conduct internal audits
✔ Maintain logs
✔ Maintain KYC & PAN records
✔ Provide tax proofs
✔ Ensure program integrity
✔ Handle law enforcement requests

VCQRU will only:

✔ Provide system data
✔ Provide logs upon written brand authorization

VCQRU is NOT part of audit interaction unless legally required.

14.0 OVERVIEW

This section defines:

✔ How a brand can exit
✔ How VCQRU can terminate service
✔ What obligations both parties have
✔ What happens to unresolved payouts
✔ What happens to user & program data
✔ Post-termination liabilities
✔ Data retention & deletion rules

VCQRU's objective is to ensure a safe, legally protected, and financially settled exit.

14.1 TYPES OF TERMINATION

Termination can occur:

✔ By Brand (Voluntary Exit)

Brand decides to close the program or end the relationship.

✔ By VCQRU (For Cause)

VCQRU may terminate if Brand:

- Fails to pay dues
- Violates program rules
- Uses system illegally
- Commits fraud or misuse
- Violates data protection rules
- Damages VCQRU reputation
- Breaks compliance laws
- Misrepresents scheme legality

✔ By Mutual Agreement

Both parties can choose to discontinue.

14.2 NOTICE PERIOD

Unless otherwise agreed in the MSA:

✔ Brand must provide 30 days written notice
✔ VCQRU must provide 30 days notice (if termination not for cause)

For fraud or illegal activity:

VCQRU may terminate immediately.

Without notice.

14.3 BRAND MUST CLEAR ALL FINANCIAL DUES BEFORE TERMINATION

Brand must fully clear:

✔ Pending VCQRU invoices
✔ Platform usage fees
✔ Program-specific charges
✔ SMS/WhatsApp bills
✔ AWS/server expenses (if applicable)
✔ Custom development charges
✔ Pending payout wallet top-up
✔ TDS dues (Section 194R)
✔ Any outstanding user benefits
✔ Any penalties or misuse fees

VCQRU will NOT proceed to data export or exit process until all dues are settled.

14.4 BRAND MUST CLEAR ALL USER PAYOUTS BEFORE TERMINATION

The Brand must:

✔ Clear all pending cashbacks
✔ Clear all pending points redemptions
✔ Clear all locked payouts due to KYC
✔ Clear all pending TDS-related adjustments
✔ Close all unsettled disputes
✔ Reprocess all failed payouts
✔ Resolve any user claims

VCQRU has **no liability** for:

❌ Missed payouts
❌ Abandoned users
❌ Negative reviews
❌ Consumer complaints

Brand owns all liabilities.

14.5 BRAND MUST HANDLE ALL POST-TERMINATION USER COMPLAINTS

After termination:

Brand must continue to handle:

✔ Product authenticity complaints
✔ Counterfeit reports
✔ Cashback-related grievances
✔ KYC-related issues
✔ Reward & points disputes
✔ Legal notices filed by customers
✔ Consumer court cases

VCQRU will NOT provide support to end-users post termination.

14.6 DATA HANDLING DURING EXIT

VCQRU will:

✔ Provide data summary if requested
✔ Provide program-level logs
✔ Provide payout history
✔ Provide scan data
✔ Provide fraud alerts
✔ Provide KYC logs (if applicable)
✔ Provide TDS-related logs (if provided by brand)

VCQRU will NOT provide:

❌ Full raw database
❌ Infrastructure access
❌ Backend access
❌ Server credentials
❌ Source code
❌ Proprietary fraud engine data
❌ System architecture

Only program-specific data is shared.

14.7 DATA RETENTION & DELETION RULES

After program ends:

VCQRU retains data only for legally allowed duration under:

- DPDP Act
- IT Act
- Tax compliance rules
- Audit requirements

- Anti-fraud retention

Retention includes:

✔ Scan data
✔ Transaction logs
✔ Payout logs
✔ Device fingerprints
✔ Fraud flags
✔ KYC approvals/rejections

After retention period:

✔ Data is securely deleted OR
✔ Permanently anonymized

Brand CANNOT demand immediate deletion — compliance laws mandate retention.

14.8 BRAND RESPONSIBILITY FOR POST-TERMINATION LEGAL & TAX ISSUES

Brand must:

✔ Handle TDS notices
✔ File remaining returns
✔ Provide Form 16A (if pending)
✔ Clear tax liabilities
✔ Maintain KYC/PAN audit records
✔ Provide compliance proofs to authorities
✔ Handle consumer court claims
✔ Manage counterfeit disputes

VCQRU is NOT involved after termination.

14.9 VCQRU RIGHT TO TERMINATE IMMEDIATELY (FOR CAUSE)

VCQRU may terminate without notice if Brand:

✔ Misuses data
✔ Performs illegal or unethical activity
✔ Violates TDS/GST compliance
✔ Runs fraudulent schemes
✔ Misuses program for money laundering
✔ Fails to pay dues for more than 45 days
✔ Damages VCQRU reputation publicly
✔ Attempts to reverse-engineer the platform
✔ Uses system outside agreed scope
✔ Violates end-user privacy laws

In such cases:

🟥 **No refund or partial refund is applicable.**

🟥 **VCQRU may pursue legal action if required.**

14.10 NO REFUND POLICY

Brand acknowledges:

✔ VCQRU does not provide refunds for pre-paid service fees
✔ No refunds for partially used subscription periods
✔ No refunds for marketing/communication spent
✔ No refunds for program setup fees
✔ No refunds for custom development
✔ No refunds for server/SMS/API consumption

This is industry standard.

14.11 INTELLECTUAL PROPERTY PROTECTION

Upon termination:

✔ VCQRU retains ownership of:

- Source code
- Database structure
- APIs
- Dashboards
- Anti-fraud engine
- Smart labeling technology
- Patented/Nano-optical technologies
- System libraries
- Admin panel
- Reports & analytics engine

Brand has NO rights to:

❌ Duplicate
❌ Reproduce
❌ Reverse-engineer
❌ Reuse
❌ Modify

VCQRU technology.

14.12 TERMINATION CERTIFICATE

After successful exit:

VCQRU issues:

✔ Program Closure Certificate
✔ Data Export Confirmation
✔ Wallet Reconciliation Summary
✔ Compliance Checklist (optional)

Brand must sign:

✔ Exit Acceptance
✔ No-Pending-Dues Declaration
✔ No-Pending-Payouts Declaration
✔ No-Legal-Claims Declaration
✔ No-Further-Support Requirement

This closes the relationship safely.

BATCH 15 — FINAL ACCEPTANCE, AUTHORITY & AGREEMENT POLICY

(The official binding & closing section — legally enforceable)

15.0 OVERVIEW

This batch confirms:

✔ Brand has read, understood & accepted all policies
✔ Brand accepts full responsibility for their program
✔ VCQRU is only a technology provider
✔ All disputes, liabilities, compliance, penalties stay with Brand
✔ Brand cannot shift accountability to VCQRU in future
✔ Only written approvals matter
✔ All verbal commitments are invalid

15.1 BRAND ACCEPTANCE & ACKNOWLEDGEMENT

The Brand hereby acknowledges and agrees that:

🟩 **The entire policy (Batch 1 to Batch 15) is understood in full.**

🟩 **The Brand has reviewed all responsibilities & obligations.**

🟩 **The Brand accepts all liabilities mentioned.**

🟩 **The Brand agrees that VCQRU is only a technology enabler.**

🟩 **No part of this policy can be disputed later.**

15.2 AUTHORITY CONFIRMATION

Brand confirms that:

✔ The person signing this agreement is legally authorized
✔ Signing authority has full power to bind the Brand
✔ The Brand accepts all risks, responsibilities & liabilities
✔ VCQRU can rely on decisions made by this authorized signatory

If an unauthorized person approves changes, Brand still remains fully responsible.

15.3 WRITTEN APPROVALS ONLY (NO VERBAL PROMISES ALLOWED)

Brand agrees that:

✔ Only written, email-approved instructions are valid
✔ Verbal, WhatsApp, phone, meeting room discussions are NOT valid approvals
✔ No unofficial commitments from Brand sales/marketing teams will be considered

VCQRU will follow ONLY written confirmations.

15.4 ENTIRE AGREEMENT CLAUSE

This document:

✔ Overrides ALL previous verbal or written communication
✔ Supersedes emails, chats, and discussions
✔ Is the ONLY valid agreement regarding the program

Nothing outside of this can be used legally to claim liability.

15.5 NO MODIFICATION WITHOUT WRITTEN CONSENT

Brand agrees:

✔ No program rule will be modified without written request
✔ No operational point will be changed verbally
✔ Any change must include:

- Written request
- Approval hierarchy
- Impact analysis approval
- Updated SOP
- Updated T&C (if applicable)

This maintains full auditability.

15.6 BRAND ACCEPTS FULL LIABILITY FOR:

✔ Program rules

✔ Reward structure

✔ User eligibility

✔ KYC & PAN handling

✔ TDS compliance

✔ Counterfeit product claims

✔ Payout errors

✔ Supply chain misuse

✔ Scheme miscommunication

✔ Legal disputes

✔ Audit findings

✔ User complaints

✔ Fraud loss

✔ All financial losses

VCQRU retains ZERO liability for these items.

15.7 NO LIABILITY FOR VCQRU BEYOND PLATFORM FEES

Brand agrees and acknowledges that:

✔ VCQRU’s maximum liability is ONE MONTH of platform fee
✔ No consequential damages may be claimed
✔ No brand loss, profit loss, fraud loss can be claimed
✔ No reputational damage claims will be entertained
✔ No brand-supplier or retailer disputes can be extended to VCQRU

This ensures COMPLETE legal protection.

15.8 NON-DISPARAGEMENT CLAUSE

Brand agrees:

✔ Not to publicly defame VCQRU
✔ Not to publish misleading allegations
✔ Not to blame VCQRU for brand-side failures
✔ Not to damage VCQRU’s reputation in any forum (online or offline)

Violation allows VCQRU to seek legal recourse.

15.9 CONFIDENTIALITY AGREEMENT

Brand must keep secret:

✔ VCQRU platform architecture
✔ Business logic
✔ APIs
✔ Fraud engine details
✔ Admin dashboards
✔ Financial models
✔ User & device data
✔ Security protocols
✔ Patented/Nano-optical technology details

Disclosure without permission is a legal breach.

15.10 AGREEMENT EFFECTIVE DATE

This agreement becomes active on:

✔ Date of Brand’s written acceptance
✔ Date of first invoice payment
✔ OR date of first program launch

Whichever occurs earliest.

15.11 RENEWAL TERMS

If not terminated:

✔ The agreement auto-renews annually
✔ Renewal fees apply
✔ Platform usage fees continue
✔ All policies remain unchanged unless mutually amended

15.12 GOVERNING LAW, ARBITRATION & JURISDICTION

Brand agrees:

✔ Indian Contract Act applies
✔ DPDP Act applies
✔ IT Act applies
✔ Tax & TDS laws apply
✔ Arbitration will be in **Gurugram, Haryana**
✔ Final legal jurisdiction: **Gurugram Courts** only

No other courts or jurisdictions are acceptable.

15.13 SIGNATURE & STAMPING

Brand must provide:

✔ Company stamp
✔ Authorized signatory name
✔ Designation
✔ Date
✔ Full signature

VCQRU will countersign and retain a copy for compliance.