RBC Clear Security Procedures

How We Protect Your Treasury Operations

Introduction

This document explains the standard security procedures that RBC Clear implements to mitigate risks to your treasury data and payments through multiple layers of protection, including data encryption, access controls and entitlements, business rules, transaction limits, and comprehensive audit trails. It is important that you read these security procedures carefully as you are deemed to have accepted them when you sign the Relationship Documents, or if you utilize them after they have been updated. If we have agreed to bespoke security procedures with you, those will be documented separately.

This document addresses:

- Data protection across all RBC Clear channels (Portal, H2H, Swift)
- Access controls, entitlements and role-based permissions
- Authentication procedures and authorization requirements
- Business rules and transaction limits by payment type
- Dual approval requirements and segregation of duties
- Account change procedures (beneficiary updates, compliance information, contact details)
- Fraud detection and monitoring
- Complete audit trail and transaction history
- Payment-type security controls (ACH, FX, DACA, Time Deposits, Swift)

What this document does NOT cover:

- Operational step-by-step procedures (see our How-To guides)
- Detailed compliance certifications and audit reports (see our Legal and Privacy & Security sections)
- Incident response procedures (see our Security Incident Response Policy)
- Technical architecture and infrastructure details

For Operational procedures:
Step-by-step procedures for enrollment, configuration and daily operations are available in our How-To guides.
To access RBC Training Resources in the RBC Clear Marketing gated site, complete this form.

For Legal and Privacy and Security policies:
Detailed legal and privacy policies, security certifications, and compliance information are available in the Legal and Privacy & Security links in the footer at rbcclear.com.

Table of Contents

Authentication and Access

For: All Users | Entitlements: Universal

Getting Started Safely

Security is built-in from day one, so your team has the appropriate access, data is encrypted and every action is auditable.

What We Do

- Create secure login credentials with mandatory multi-factor authentication (MFA) via email verification links and phone (SMS or voice call with one-time PIN) to mitigate unauthorized access
- Provide you the tools to create rules that prevent the same person from having the ability to both initiate and approve payments
- Encrypt all data using AES-256 (Advanced Encryption Standard with 256-bit key) to mitigate risk if data is exposed
- Provide integration testing capability to help prevent errors before going live with real payments
- Maintain detailed audit logs of every action to support accountability and monitor client behavior

What You Can Do

- Create strong passwords to mitigate brute-force attacks
- Assign permissions by job function (such as uploads for operations and large-amount approvals for CFOs) to limit the potential for compromised accounts
- Immediately revoke access when employees leave to avoid unauthorized access from former employees
- Protect SSH keys if using SFTP (Secure File Transfer Protocol) to prevent unauthorized use of your connectivity
- Immediately report suspicious access attempts to enable investigation of potential security concerns

Verify Every Login

Every login requires a password and an MFA verification code delivered via email or phone to reduce the risk of unauthorized access.

What We Do

- Require username (corporate email) and password at every login to establish initial identity verification
- Accept Terms and Conditions on first login
- Support secure first-time login via verified email links to enable new users to activate accounts
- For every login, send MFA verification codes via phone (SMS or voice call with one-time PIN) to protect against password-only attacks
- For first-time login, send a secure email link where users set up a temporary password (not pre-generated PIN) to reduce password exposure risks during account creation
- Track all login attempts (successful and failed) to help identify potential unauthorized access attempts
- Alert you to account lockout to flag potential security concerns
- Check that the log-in attempt is not from blacklisted countries

What You Can Do

- Use your corporate email as username to verify employment and link access to your organization
- Enable mandatory MFA to add a second verification layer
- Never share your password, even with support staff, to avoid unauthorized access
- Change your password regularly; change it immediately if you suspect it has been compromised

Control Access by Function

Function-based access (Viewer, Creator, Approver, Administrator) so that each person has what they need—no more, no less—to limit the potential impact if an account is compromised.

What We Do

- Provide flexible permission levels (View File, View Transaction, Upload File, Approve File, Technical Integration Manager) with account-level and payment-type-level granularity to so you can match permissions to job responsibilities
- Allow you to assign permissions by person and by payment profile so users only have access to necessary functions
- Require mandatory maximum per-transaction approval limits for all users with Approver role; optionally set maximum per-day limits that must be more than or equal to maximum per-transaction limits, so approvers don't exceed their authority
- Support transaction-type-level restrictions (e.g., can approve Wires but not ACH) so users access only the payment types they need
- Support account-level restrictions so that users can only manage assigned accounts
- Support File Profile-level restrictions to maintain separation between upload and approval functions
- Enforce segregation of duties so that no single person can both initiate and approve payments.
- Log all permission changes to provide accountability
- Require dual approval for permission changes to reduce the risk of unauthorized access grants
- Prevent administrators from approving their own entitlement changes to maintain accountability
- Revoke access immediately when someone leaves to prevent unauthorized access

What You Can Do

- Assign permissions based on job role so that each person has only what they need
- Set mandatory per-transaction approval limits for all approvers to establish clear authorization boundaries
- Optionally set maximum daily limits (must be equal to or more than per-transaction limits) to add additional control
- Review and update permissions when people leave roles to keep access rights current

User & Entitlement Management

For: Administrators | Entitlements: Core Onboarding & Administrator

Onboard Securely

Onboarding requires defined authorization steps with proper verification so that we confirm we are working with authorized representatives.

What We Do

- Guide you through structured onboarding to establish proper authorization and confirm authorized representatives
- Collect documentation to verify proper authorization
- Identify Signers and Administrators upfront to document who has legal authority
- Require electronic signatures on agreements to create auditable documentation
- Send email confirmations at each milestone to keep you informed of progress
- Set up email procedures that ensure proper processing and secure sharing of information
- Enforce Entity Onboarding permissions hierarchy for proper sequencing of account setup

What You Can Do

- Identify individuals authorized to sign agreements (senior finance/treasury personnel) to establish clear responsibility
- Provide Board Resolution or Designation of Authority to verify proper authorization.
- Designate backups for administrators (typically 1-2 people) managing technical setup and access control for continuity
- Review agreements carefully, since you're committing to our security practices
- Verify all information is correct before final activation to prevent requiring re-verification later

Create a New User

Creating a new user requires corporate email verification, entitlements specification, and dual approval to prevent unauthorized account creation.

What We Do

- Collect corporate email as username to establish identity verification
- Require entitlements specification (account-level, payment-type-level, currencylevel and method type approval limits) before activation
- Enable first-time secure login via email link where new user sets temporary password to reduce password exposure risks during account creation
- Require dual approval to reduce the risk of unauthorized access grants
- Log user creation with audit trail to provide accountability

What You Can Do

- Collect corporate email address for new user to verify employment and link to organization
- Specify entitlements matching job role to maintain appropriate access
- Set mandatory per-transaction approval limits if user will approve payments
- Provide new user's phone number for MFA setup to enable second-factor authentication
- Verify all information before submission to prevent errors
- Understand approval timeline before new user can access the system

Sending Data and Documents via Email

RBC encrypts sensitive and confidential content within your emails for protection and security between an employee and external recipient.

What We Do

- Set up secure email procedures that allow RBC customers to receive and reply to encrypted email messages from RBC Clear
- Require Account Managers use secure email for exchange of documents or data

What You Can Do

- Check that the email has the prefix RBC Secure Email in the subject line, which indicates that the email was protected with encryption during delivery
- Do not use unsecured email for exchange of information or documents
- Promptly notify RBC Clear if any Authorized Representatives have a change of mailing or email address or other contact information

Revoke or Un-revoke User Access

Revoking access is an immediate security action removing all user access when employment ends or roles change to reduce unauthorized access.

What We Do

- Provide immediate revocation option removing all access to reduce unauthorized access
- Require reason capture for revocation to document decision rationale
- Provide Un-revoke option to reverse accidental revocations
- Log all revocations and un-revocations with audit trail to provide accountability
- Deactivate all sessions immediately upon revocation to prevent continued access

What You Can Do

- Provide clear reason for revocation to document decision
- Immediately revoke access when someone leaves or changes roles to prevent unauthorized access window
- Understand revocation is immediate and complete (user loses all access)
- Contact us immediately if accidental revocation occurs to enable quick restoration
- Notify affected teams that user's access was removed so responsibilities can be reassigned

Reset an Expired Password

Password expiration and reset procedures enforce credential rotation and mitigate risks from aging credentials.

What We Do

- Monitor password expiration to track credential age
- Enforce password history (past 8 passwords) to reduce circular reuse risks
- Send expiration warnings to enable advance notice
- Support password reset via email link for secure credential change
- Invalidate all existing sessions after reset to prevent concurrent session attacks
- Require MFA during reset to verify identity

What You Can Do

- Change password regularly and before expiration to maintain current credentials
- Use strong passwords (12 or more characters: uppercase, lowercase, numbers, symbols) to mitigate brute-force attacks
- Never reuse old passwords to prevent compromised credentials from being reactivated
- Update password immediately if compromise suspected to prevent ongoing unauthorized access
- If locked out, contact Account Manager for expedited reset

Payment Security and Controls

For: Payment Initiators and Approvers | Entitlements: Creator, Approver, File Services

Choose Your Payment Method

All payment methods use identical encryption and dual approval requirements.

What We Do

- Portal Entry: Provide Money Movement Hub for entering individual payment details and payment templates with real-time validation and approval routing
- File Upload: Accept batch files via Portal File Upload and H2H; validate in seconds with confirm receipt status: immediate acknowledgment (ACK) that file was accepted or non-acknowledgment (NACK) that file was rejected with instructions on how to correct
- Swift Messaging: Support SwiftFIN/FINplus messaging for international payments through banking networks after RMA (Relationship Management Agreement) setup
- Encrypt data end-to-end for all methods for consistent data protection regardless of your chosen pathway
- Use file naming conventions as routing and validation controls to link files to your configuration and prevent misrouting
- Support optional PGP encryption for ultra-sensitive batches for additional security layers beyond standard encryption
- Generate unique RBC file reference IDs for all outbound files to enable you to verify authenticity

What You Can Do

- Choose the method fitting your workflow based on your volume and frequency
- If using H2H, keep SSH keys secure using group email for technical contacts so that your connection isn't dependent on one person
- Follow file naming format exactly so that files route correctly and validate properly
- Test H2H connectivity in test environment with sample data before processing real payments to identify setup issues
- Verify unique RBC file reference IDs on outbound ACK/NACK files match your submission records to confirm authenticity

Set Payment Limits and Validation Rules

You set guardrails defining payment limits and validation strictness to reduce the risk of unauthorized or unusual payments processing.

What We Do

- Let you set per-transaction limits and daily approval limits by payment type and amount so that large payments receive appropriate review
- Let you define rejection thresholds (up to 100%) for all file-based payments, to match your tolerance for transaction failures
- Allow you to choose the validation level that matches your workflow needs
- Enforce limits automatically to prevent payments exceeding configured thresholds
- Show real-time usage to enable you to monitor daily limits
- Automatically delay large ACH payments over $1 million to the next business day to reduce fraud risk

What You Can Do

- Define daily limits matching your business model so that controls match your risk approach
- Choose how to validate your workflow for each payment type to support your operational needs
- Set file-based rejection thresholds based on your tolerance for failed transactions to balance error detection and processing speed
- Monitor daily usage to identify unusual patterns
- Adjust daily limits when your business changes so that controls remain appropriate

Require Maker/Checker for Every Payment

One person initiates, a different person approves. The system prevents the same person from doing both, which catches mistakes and makes fraud harder to pull off.

What We Do

- Enforce segregation of duties
- Support customizable inbound debit rules and filters for ACH and wire transactions, to enable you to control which inbound debits process automatically versus requiring review
- Show approvers all payment details needed for informed decisions
- Allow rejection with required explanation to document decision rationale
- Track every approval with full detail (who, when and action) to provide accountability
- For entitlement changes and connectivity setup, enforce maker-checker approval so that multiple people review changes
- Prevent administrators from approving their own entitlement changes

What You Can Do

- Follow control policy to allow for multiple layers of review
- If using ACH or Wire debit mandates, define rules matching your business to control which debits process automatically
- Have approvers carefully review details (total matches expectations, recipients are familiar, timing is normal) before approving to catch anomalies
- Reject anything that looks wrong to prevent questionable payments
- For entitlement requests or connectivity changes, request different users submit and approve to maintain separation of duties

Connectivity and Data Protection

For: Technical Integration Managers (TIM) | Entitlements: Technical Integration Manager

Set Up Secure Connections

Dual approval required (technician and manager sign-off) reduces the risk of misconfiguration. Connections must meet cryptographic standards and require proper authentication procedures.

What We Do

- Establish secure channels (H2H for SFTP or Swift FileAct, Swift FIN/FINplus for messaging) with encryption to meet industry standards
- Require SSH keys at minimum 2048-bit strength with supported algorithms (RSA 2048/4096, DSS 2048/4096, ECDSA, ed25519) for strong key-based authentication
- Enforce a 3-month minimum validity requirement for SSH keys, while recommending at least 6 months of validity to prevent expired credential issues
- Support optional PGP encryption for file payloads (in addition to SSH transport encryption) to add file-level protection
- For Swift connections, enforce RMA enrollment before connectivity setup to establish proper mutual agreements
- Enforce dual approval so that both technician and manager review the configuration
- Isolate test activity from production by requiring separate environments and credentials for each
- Activate connections automatically once approved with central management dashboard to provide visibility
- For Swift specify approved message types to prevent unauthorized messaging

What You Can Do

- Have technical team generate SSH keys at 2048-bit minimum for strong cryptography; check that keys have minimum 3 months of validity (6+ months recommended)
- Use group email addresses for technical contacts for continuity
- Designate a second approver for reviewing the technical setup to add oversight
- For Swift connections, submit RMA enrollment request to your Account Manager before initiating connectivity setup so that proper agreements are in place
- Keep SSH and PGP keys secure; contact your Account Manager if keys need updating to prevent unauthorized access
- Coordinate with Account Manager before production activation for proper verification

Your Data Is Encrypted and Protected

Data is encrypted whether moving or at rest, backups are encrypted and stored offsite, systems are isolated, and unauthorized access is monitored to keep your data confidential and recoverable.

What We Do

- Encrypt all data using AES-256 at rest and TLS (Transport Layer Security) 1.2+ in transit to protect data confidentiality
- Support optional PGP encryption for extra-sensitive files if you want additional layers of security
- For SFTP connections, support optional PGP file-level encryption in addition to SSH transport encryption to add file-level protection
- Keep encrypted backups offsite and test restoration regularly to support recovery from system issues
- Isolate financial systems from other systems through network segmentation to contain potential breaches
- Run regular security audits and penetration tests to identify and address vulnerabilities
- Monitor database access to detect potential unauthorized access
- Deploy Data Loss Prevention (DLP) software to reduce unauthorized data transmission
- For SFTP file transfers, prevent clients from moving, deleting or renaming files to prevent tampering

What You Can Do

- Keep encryption keys secure to prevent unauthorized decryption
- Only send data you need us to process to minimize data at risk
- Keep your own backup copies of important records to support business continuity
- If using PGP encryption, check that your PGP key has minimum 3 months validity (6+ months recommended) and complies with OpenPGP RFC 4880 to prevent key expiration
- For SFTP connections, set polling intervals at 15- to 30-minute intervals minimum to maintain system health

Managing Account Changes Securely

For: Account Administrators, Authorized Users | Entitlements: Varies By Change Type

Update User Contact Information

Your phone number and email are critical to your account security—this is how you receive MFA verification codes. If this contact information becomes outdated or incorrect, you risk losing access to your account.

What We Do

- Require MFA verification before allowing contact information changes to protect account ownership
- Send confirmation link to current email before new email activates
- Maintain change audit trail to provide transparency
- Lock account if user cannot verify current email/phone to support recovery options
- Provide Account Manager escalation if user locked out to support account recovery
- Allow user to register backup phone/email during setup to provide redundancy

What You Can Do

- Update your phone number if you change phones to maintain access to your MFA channel
- Confirm email change via verification link so that you control the change
- Understand that MFA remains active on old phone until new number confirmed so there's overlap time
- If you lose access to current phone/email, contact Account Manager immediately to regain access
- Register backup phone/email during initial setup to provide redundancy
- Notify your administrator of any contact changes

Update Beneficiary Details for Wire Recipients, ACH Information

Beneficiaries are recipients of money you send. Fraudsters often try to redirect payments by adding themselves as new recipients or modifying existing beneficiary bank details. Safeguards help catch unauthorized beneficiary changes before payments are made.

What We Do

- Require dual approval for beneficiary additions or modifications to reduce the risk of unauthorized payment diversion
- Verify beneficiary bank information against banking databases to reduce data entry errors
- Show confirmed bank name and address to enable you to verify the destination
- Maintain complete change history to provide audit capability
- Allow 24-hour effective date delay for new beneficiaries to catch unauthorized additions
- Require Account Manager verification for high-risk countries to meet compliance requirements
- Send notification to payment approvers when beneficiary list changes to keep teams informed
- Flag payments to new beneficiaries for enhanced review to add oversight

What You Can Do

- Add beneficiaries only through authorized procedure to maintain control
- Verify beneficiary bank details before submission to reduce misrouting
- Understand new beneficiaries have 24-hour waiting period to catch unauthorized additions
- Notify your payment approvers when new beneficiaries are added to maintain awareness
- Review beneficiary changes periodically to monitor for unauthorized activity
- Report suspicious changes to Account Manager immediately to support investigation
- Do not add beneficiaries on behalf of other users to maintain accountability

Glossary of Terms

ACH (Automated Clearing House): Electronic network for batch payments in the U.S., used for payroll, vendor payments and recurring transfers. Supports credit and debit transactions via multiple entry class codes (CCD, CTX, PPD).

AES-256: Advanced Encryption Standard using a 256-bit key; military-grade encryption standard used for data at rest.

API (Application Programming Interface): Software tool allowing applications to communicate with each other.

ABA Routing Number: Nine-digit code identifying a U.S. bank branch required for domestic wire and ACH transfers.

Audit Trail: Complete record with timestamps of who did what and when; cannot be altered.

Authorization: Legal documentation (Board Resolution or Designation of Authority) confirming an organization is authorized to use RBC Clear services.

Batch Level Rejection: Validation approach where only failed transaction batches are rejected; successfully validated batches process normally.

Beneficiary: Payment recipient (individual or business).

BIC/Swift Code: Bank Identifier Code for international banks in Swift messaging. This is similar to ABA routing for international transfers.

Board Resolution: Official organizational document authorizing specific individuals to act on behalf of the organization.

Book Transfer: Payment between your own RBC Clear accounts within the same-day processing window.

Business Continuity: Ability to continue operating and recover data after disaster through encrypted offsite backups.

CAMT: Cash Management format; ISO 20022 standard format for machine-readable bank statements (CAMT.052, CAMT.053, CAMT.054).

Connectivity Profile: Secure connection between your systems and RBC Clear supporting Host-to-Host, Swift FIN, Swift FINplus, or Swift FileAct channels.

Control Totals: Summary numbers for payment batches (total debits, total credits, transaction count) used to verify file contents.

Cutoff Time: Deadline for payment processing. These times are communicated to the customer by the bank.

DACA (Deposit Account Control Agreement): Tri-party agreement between customer, secured creditor and bank allowing creditor to perfect security interest in customer's depository account. There are 2 types of DACAs:

- **Blocked:** Account holder cannot transact
- **Springing:** Account holder transacts freely until creditor issues Notice of Exclusive Access.

DLP: Data Loss Prevention software detecting and blocking unauthorized sensitive data transmission outside our system.

Designation of Authority: Organizational document delegating specific authority to individuals to act on behalf of the organization.

Digital Signature: Electronic verification of document authenticity and signer identity.

Dual Approval: Security check requiring 2 people be involved in a decision or transaction.

- The Maker creates the request.
- The Checker approves the request.
- Cannot be bypassed by the same user.

Entitlements: User permissions (View File Level, View Transaction Level, Upload File, Approve File, Technical Integration Manager, etc.) that are role-based and system-enforced.

File Level Rejection: Most restrictive validation approach where, if any transaction fails, entire file is rejected.

File Profile: Configuration defining how payment files are validated specifying transaction types allowed, error handling, limits and rejection thresholds.

File Reference ID: Unique identifier assigned by RBC Clear to all outbound files enabling clients to verify authenticity.

Fraud Detection: Machine learning monitoring all payments 24/7 for unusual patterns; flags suspicious activity for investigation.

FX (Foreign Exchange): Cross-currency payments allowing you to send and receive payments in multiple currencies. Supports customizable transaction limits and cumulative daily limits.

GDPR (General Data Protection Regulation): EU data protection regulation with which we align.

H2H (Host-to-Host): Connection method using SFTP for batch payment submission.

ISO 20022: International standard for electronic data interchange between financial institutions.

ISO XML: Extensible Markup Language format for payment files compliant with ISO 20022 pain standards.

MFA (Multi-factor authentication): Verification using 2 or more factors which could include a password, a code or a fingerprint scan.

Mandate: ACH Debit mandate; customizable rules and filters clients establish to control which inbound ACH direct debit transactions are automatically accepted, rejected, or flagged for manual review.

NACK (Non-Acknowledgment): Rejection of submitted file with detailed explanation of validation failures.

PCI DSS (Payment Card Industry Data Security Standard): Industry security standard for handling payment card data.

PGP (Pretty Good Privacy): Additional encryption layer for extra-sensitive file batches, providing encryption on top of standard AES-256 and TLS protections.

PIPEDA (Personal Information Protection and Electronic Documents Act): Canada's privacy law.

PSR (Payment Status Report): Displays successful transactions, failed transactions, and reasons for failures.

Rejection Threshold: For ACH file uploads, configurable percentage (0–100%) of failed transactions at which the entire file is rejected.

RMA (Relationship Management Agreement): Enrollment and security agreement required for Swift FIN/FINplus connectivity.

SFTP (Secure File Transfer Protocol): Uses SSH encryption for secure batch payment transmission.

SOC 2 (Service Organization Control 2): Audit standard verifying security controls.

rbcclear.com