

LAKELAND HOUSING AUTHORITY**COMPREHENSIVE CASH HANDLING, RECEIPTS,
BANKING AND DISBURSEMENT POLICY****Fiscal Year 2027***Cash • Checks • Cards • ACH/EFT • Wires • Online Banking • Fraud Controls*

Policy Item	Information
Agency	Housing Authority of the City of Lakeland, Florida
Resolution	26-1575
Board Meeting / Effective Date	09/21/2026
Board Chairman	David Samples
Executive Director	Benjamin Stevenson
Policy Owner	Director of Finance under Executive Director oversight
Supersedes	Prior cash handling SOPs, including 2025/2026 versions

POLICY STATUS

This comprehensive final policy replaces the prior framework document. It establishes detailed controls for physical receipts, electronic payments, banking access, disbursements, reconciliations, ACH fraud monitoring, cybersecurity, incident response, records, training, and audit readiness.

Approval	Signature / Date
Board Chairman	David Samples Signature:  Date: 09/21/2026
Executive Director	Benjamin Stevenson Signature:  Date: 09/21/2026

Executive Transmittal and Board Action

To	Board of Commissioners
From	Benjamin Stevenson, Executive Director
Subject	FY 2027 Comprehensive Cash Handling, Receipts, Banking and Disbursement Policy
Requested Action	Approve under Resolution 26-1575; authorize implementation and non-substantive technical updates.
Board Meeting	09/21/2026

BOARD MOTION

Approve the FY 2027 Comprehensive Cash Handling Policy under Resolution 26-1575, effective 09/21/2026, and authorize the Executive Director or designee to implement procedures, banking controls, training, and corrective actions.

Table of Contents

1. 1. Purpose, Authority, Scope, and Order of Precedence
2. 2. Definitions
3. 3. Governance, Delegation, and Accountability
4. 4. Internal Control Framework and Segregation of Duties
5. 5. Authorized Collection Channels
6. 6. Cash, Check, and Money Order Receipts
7. 7. Deposits, Transport, and Remote Deposit
8. 8. Credit Cards, Payment Portals, and Merchant Services
9. 9. ACH and EFT Origination and Receipt Controls
10. 10. Wire Transfers and Real-Time Payments
11. 11. Vendor and Employee Banking Changes
12. 12. Bank Accounts, Signatories, and Online Access
13. 13. Disbursements, Checks, Positive Pay, and Stop Payments
14. 14. Reconciliations, Cash Position, and Federal Funds
15. 15. Petty Cash, Change Funds, and Cash Boxes
16. 16. Physical Security and Business Continuity
17. 17. Cybersecurity, Fraud Prevention, and Incident Response
18. 18. Refunds, Returned Items, Chargebacks, and Unclaimed Funds
19. 19. Records, Privacy, Retention, and Audit
20. 20. Training, Monitoring, Compliance, and Discipline
21. 21. Implementation and Revision Control
22. Appendix A. Segregation of Duties Matrix
23. Appendix B. Daily Cash Closeout
24. Appendix C. Deposit Checklist
25. Appendix D. ACH/Wire Authorization
26. Appendix E. Banking Change Verification
27. Appendix F. Reconciliation Checklist
28. Appendix G. Fraud Incident Checklist
29. Appendix H. Annual Control Dashboard

1. Purpose, Authority, Scope, and Order of Precedence

This policy safeguards LHA funds, establishes reliable financial reporting, supports compliance with federal awards and HUD requirements, and applies to all employees, commissioners, agents, properties, programs, instrumentalities, contractors, and service providers that receive, handle, transmit, approve, record, reconcile, or oversee LHA funds or banking information.

- 2 CFR 200.302 and 200.303 financial management and internal-control requirements.
- Federal award, HUD, MTW, HCV, Public Housing, grant, lender, investor, and banking requirements.
- Florida public records, unclaimed property, fraud, ethics, and other applicable laws.
- Nacha Operating Rules and LHA banking agreements for ACH activity.
- LHA Procurement Policy, records schedules, cybersecurity standards, budgets, delegations, and Board resolutions.

2. Definitions

Term	Definition
ACH	Automated Clearing House electronic transfer.
Dual control	Two authorized people perform or approve separate parts of a transaction.
EFT	Electronic transfer of funds, including ACH and other approved methods.
Positive Pay	Bank service that compares presented checks or electronic debits with authorized data.
Remote deposit	Electronic deposit of check images through an approved bank service.
Sensitive banking information	Account, routing, credential, token, file, payment instruction, or authentication data requiring restricted access.
Wire transfer	Same-day or rapid transfer through an approved bank network.

3. Governance, Delegation, and Accountability

Role	Responsibility
Board	Adopts policy and receives material incident or audit reporting.
Executive Director	Executive accountability, bank authority, delegations, emergency approvals, corrective action.
Director of Finance	Policy administration, banking, cash management, reconciliation, monitoring, training, incident coordination.
Department Directors	Written departmental procedures, staffing controls, security, timely deposits, corrective action.
Cash Handlers	Accurate receipt, safeguarding, documentation, timely transfer, and incident reporting.
Reconcilers/Approvers	Independent review, exception investigation, certification, and escalation.
IT/Security	Access controls, MFA, logging, cybersecurity, continuity, and incident support.

4. Internal Control Framework and Segregation of Duties

LHA will establish, document, maintain, evaluate, and promptly correct internal controls. Collection, custody, deposit preparation, recording, authorization, release, reconciliation, and master-file maintenance should be separated. When staffing prevents full separation, management must document compensating review controls.

- No person may approve a payment to themselves.
- No person who creates or changes vendor banking data may independently release the related payment.
- Bank reconciliations must be prepared independently of routine cash receipt and disbursement functions when practicable.
- Shared credentials and generic banking accounts are prohibited.
- Transactions may not be split to avoid approval or dual-control thresholds.

5. Authorized Collection Channels

Channel	Control Standard
Cash	Only at specifically authorized locations and hours; minimize use.
Checks/money orders	Payable to LHA or approved entity; restrictively endorse promptly.
Cards/portal	Approved processor and portal; no storage of full card data by staff.
ACH/EFT	Approved account and instructions; validation, authorization, monitoring, and reconciliation.
Lockbox/remote deposit	Bank-approved arrangement with daily reporting and duplicate-deposit controls.

6. Cash, Check, and Money Order Receipts

- Issue a sequential or system-generated receipt showing date, amount, payer, purpose, method, and handler.
- Count cash in a secure nonpublic area; verify totals by a second person when required.
- Never leave currency, checks, or money orders unattended or visible.
- Restrictively endorse checks immediately or as soon as operationally practicable.
- Do not accept postdated, altered, unsigned, stale-dated, third-party, or otherwise questionable items without Finance approval.
- Balance receipts to the system, cash drawer, checks, money orders, and daily closeout report.
- Gifts or donations in cash may be accepted only through an authorized Finance process.

7. Deposits, Transport, and Remote Deposit

Receipts will be deposited intact and promptly, normally the same business day when practicable. Cash received after cutoff shall be secured and deposited the next business day. Cash must not be used to pay expenses, cash checks, make loans, or replenish petty cash.

- Use tamper-evident bags or locked containers where appropriate.
- Maintain chain-of-custody documentation.
- Vary transport timing and routes when security warrants.
- Remote-deposit users must prevent duplicate deposit and securely destroy checks only after bank acceptance and the approved retention period.
- Deposit documentation must reconcile to receipts and bank credit.

8. Credit Cards, Payment Portals, and Merchant Services

- Use approved processors and contracts.
- Do not write, email, photograph, or retain full card numbers or security codes.
- Restrict refunds to authorized staff and the original payment method when practicable.
- Review daily settlement, processor fees, chargebacks, failed payments, and portal exceptions.
- Complete merchant-access reviews at least annually and upon personnel changes.
- Do not key card data received through insecure email or voicemail.

9. ACH and EFT Origination and Receipt Controls

2026 NACHA UPDATE

All non-consumer ACH originators are subject to risk-based processes and procedures intended to identify potentially fraudulent ACH transactions under NACHA's 2026 rule changes. LHA will document, implement, train on, and review its ACH fraud-monitoring process at least annually and when risk changes.

- Require documented authorization, proper account coding, available funds, and dual approval before release.
- Use bank templates with restricted edit rights; review changes independently.
- Apply transaction and daily limits appropriate to risk.
- Verify new or changed banking information through a trusted contact method independent of the request.
- Use prenotes, micro-entries, account validation, or bank services when appropriate.
- Monitor unusual amounts, frequency, first-time payees, dormant vendors, rapid changes, duplicate files, and out-of-pattern activity.
- Review returns, reversals, notifications of change, rejected files, and suspicious bank notices promptly.
- Retain ACH files, approvals, validations, exception reviews, and annual rule/audit evidence.

10. Wire Transfers and Real-Time Payments

- Use only when operationally justified and approved.
- Require initiator and separate approver; high-risk or exceptional transfers require Finance leadership or Executive Director approval under delegation.
- Independently verify destination instructions and purpose.
- Review beneficiary, bank, amount, timing, sanctions or bank warnings, supporting invoice/contract, and funding source.
- Confirm bank acceptance and post promptly; reconcile same day or next business day.
- Do not act on urgent payment instructions received only by email, text, or changed contact information.

11. Vendor and Employee Banking Changes

- Route changes through a controlled form or secure portal.
- Verify using a known phone number or contact already on file, not information supplied in the change request.
- Require independent review of supporting documentation and system entry.
- Apply a reasonable hold or heightened review to first payment after change.
- Send confirmation to the prior trusted contact when appropriate.
- Document failed verification and suspected impersonation.

12. Bank Accounts, Signatories, and Online Access

- Open or close accounts only with documented authority.
- Maintain an inventory of accounts, purpose, funding, signatories, services, limits, and reconciliation owner.

- Use individual credentials, MFA, least privilege, and bank tokens.
- Review users, signatories, entitlements, dormant accounts, and limits at least annually and promptly after role changes or separation.
- Prohibit saving credentials in browsers or sharing tokens.
- Enable alerts for high-value activity, new payees, profile changes, failed logins, and unusual transactions.

13. Disbursements, Checks, Positive Pay, and Stop Payments

- Pay only from approved invoices, contracts, purchase orders, reimbursement records, payroll, or other valid obligations.
- Use positive pay or comparable controls where available.
- Secure check stock, signature devices, tokens, and electronic templates.
- Prohibit pre-signed blank checks.
- Investigate stale, duplicate, altered, missing, returned, or unauthorized checks.
- Require documented stop-payment and replacement approval; confirm no prior payment before reissue.
- Void checks physically and in the system; retain required evidence.

14. Reconciliations, Cash Position, and Federal Funds

Reconciliation	Minimum Standard
Daily receipts	Receipt system to cash/checks, deposit, settlement, and exceptions.
Bank accounts	Monthly, timely, independently reviewed, with outstanding items investigated.
Merchant/portal	Daily or settlement-cycle match to processor and ledger.
ACH/wires	Bank confirmation to approved batch, ledger posting, and funding.
Federal/HUD cash	Reconcile draws, disbursements, VMS/PMS or applicable systems, general ledger, reserves, and restrictions.
Petty cash/change funds	Periodic surprise count and custodian reconciliation.

Reconciling items will be aged, assigned, investigated, corrected, and escalated. Unexplained differences, stale checks, negative balances, duplicate payments, unusual transfers, and federal cash discrepancies require prompt management review.

15. Petty Cash, Change Funds, and Cash Boxes

- Establish only by written Finance authorization with custodian, amount, purpose, location, and replenishment method.
- Keep physical funds locked and separate from personal money.
- Use original receipts and documented business purpose.
- Do not use for payroll, personal advances, loans, check cashing, or avoidance of procurement controls.
- Conduct surprise counts; report shortages or overages immediately.

16. Physical Security and Business Continuity

- Limit access to safes, drawers, cash rooms, check stock, and deposit supplies.
- Change combinations, keys, and codes after turnover, compromise, and periodically.
- Count funds away from public view and cameras or windows that expose details.

- Maintain duress, robbery, emergency, disaster, and system-outage procedures.
- Prioritize personal safety; staff should not resist a robbery.
- Restore records, banking access, approvals, and reconciliations through tested continuity procedures.

17. Cybersecurity, Fraud Prevention, and Incident Response

Risk	Preventive / Detective Control
Business email compromise	Independent call-back; dual approval; banner/warning awareness; mailbox/security review.
Credential theft	MFA, least privilege, device security, password controls, alerts.
Vendor impersonation	Trusted-contact validation and change confirmation.
Payroll redirect	Controlled employee change process and independent notification.
ACH/wire anomaly	Limits, templates, monitoring, exception review, bank alerts.
Check fraud	Secure stock, restrictive endorsement, positive pay, daily review.
Insider fraud	Segregation, leave/rotation where feasible, logs, reconciliation, surprise review.

Suspected fraud, theft, loss, data compromise, misdirection, counterfeit items, unauthorized access, or reconciliation anomalies must be reported immediately to Finance and the Executive Director or designee. LHA will contact the bank promptly, attempt recall/return/stop payment, preserve evidence, restrict access, notify IT/security, legal, insurer, law enforcement, HUD or grantors when required, and document recovery and corrective action.

18. Refunds, Returned Items, Chargebacks, and Unclaimed Funds

- Refunds require proof of original payment, entitlement, coding, approval, and duplicate-payment review.
- Return funds to the original payer and method when feasible.
- Assess returned-payment fees only when authorized.
- Track chargebacks and respond within deadlines.
- Research stale checks and unclaimed property; comply with applicable Florida requirements before escheatment.

19. Records, Privacy, Retention, and Audit

- Maintain receipts, deposit slips, bank confirmations, approvals, statements, reconciliations, payment files, check registers, merchant reports, incident records, access reviews, and training evidence.
- Retain federal award records under 2 CFR 200.334 and longer when HUD, Florida schedules, grants, audits, litigation, tax credits, bonds, or contracts require.
- Protect PII and banking data through role-based access, encryption, secure transmission, and disposal.
- Provide audit access while protecting exempt or confidential information.

20. Training, Monitoring, Compliance, and Discipline

- Train before granting cash or banking duties and at least annually thereafter.
- Require ACH, wire, BEC, phishing, vendor-change, privacy, and incident-response training for relevant staff.
- Perform periodic file review, access review, surprise cash counts, reconciliations, exception analysis, and corrective action.

- Violations may result in removal of access, restitution, discipline, termination, contract remedies, reporting, or referral consistent with law and HR policy.

21. Implementation and Revision Control

Action	Owner	Timing
Approve policy	Board	09/21/2026
Issue detailed procedures	Finance	Upon adoption
Review bank users/signatories	Finance/IT	Upon adoption and annually
Implement ACH fraud monitoring	Finance	Current and annually reviewed
Train covered staff	Finance/HR/IT	Upon assignment and annually
Review controls and incidents	Finance/Executive Director	Quarterly/annually

Revision	Date	Description	Approval
FY 2027 Comprehensive Revision	09/21/2026	Replaces framework and prior SOPs; adds electronic payment, fraud, cybersecurity, reconciliation, access, and appendices.	Resolution 26-1575

Appendix A. Segregation of Duties Matrix

Function	Initiate	Approve	Release/Custody	Record	Reconcile
Cash receipt					
Deposit					
ACH batch					
Wire transfer					
Vendor bank change					
Check issuance					
Refund					

Appendix B. Daily Cash Closeout

- ☐ Receipts sequential/system complete
- ☐ Currency counted
- ☐ Checks/money orders listed
- ☐ Card/portal settlement matched
- ☐ Drawer/cash box reconciled
- ☐ Over/short documented
- ☐ Deposit prepared intact
- ☐ Second review completed
- ☐ Funds secured/transported
- ☐ System posted

Appendix C. Deposit Checklist

- ☐ Deposit date and bank
- ☐ Receipt batch total
- ☐ Cash total
- ☐ Check/money order total
- ☐ Restrictive endorsement
- ☐ Deposit slip total
- ☐ Tamper-evident bag/chain of custody
- ☐ Bank confirmation
- ☐ Ledger posting

☐ Exception resolution

Appendix D. ACH/Wire Authorization

Field	Entry
Payment type	ACH / Wire / RTP / Other
Payee and purpose	
Amount and date	
Funding source/account	
Bank instructions verified by / method / date	
Supporting documents	
Fraud-monitoring review	
Initiator	
Independent approver	
Bank confirmation / trace	
Ledger posting / reconciliation	

Appendix E. Banking Change Verification

- ☐ Controlled request received
- ☐ Existing vendor/employee identity verified
- ☐ Trusted contact method used
- ☐ Account documentation reviewed
- ☐ Independent system-entry review
- ☐ Prior contact notified as appropriate
- ☐ First-payment heightened review
- ☐ Evidence retained

Appendix F. Reconciliation Checklist

- ☐ Statement obtained independently
- ☐ Beginning balance agrees
- ☐ Deposits matched

- ☐ Checks/disbursements matched
- ☐ ACH/wires matched
- ☐ Fees/interest posted
- ☐ Outstanding items aged
- ☐ Exceptions assigned and resolved
- ☐ Ledger adjusted with approval
- ☐ Independent reviewer certified

Appendix G. Fraud Incident Checklist

- ☐ Stop/recall/return/positive-pay action initiated
- ☐ Bank fraud unit contacted
- ☐ Accounts/credentials/tokens secured
- ☐ Executive Director and Finance notified
- ☐ IT/security and legal notified
- ☐ Evidence preserved
- ☐ Insurer/law enforcement/HUD/grantor evaluated
- ☐ Affected parties notified if required
- ☐ Loss/recovery quantified
- ☐ Root cause and corrective action documented

Appendix H. Annual Control Dashboard

Metric	Q1	Q2	Q3	Q4	Annual Action
Deposits timely					
Reconciliations timely					
Open reconciling items					
ACH/wire exceptions					
Bank access reviews					
Training completion					
Fraud/loss incidents					
Corrective actions					

FINAL IMPLEMENTATION CONTROL

Finance should insert the current banking institutions, accounts, signatory matrix, approval limits, deposit cutoffs, petty-cash

amounts, incident contacts, records retention schedule, and department-specific procedures in controlled internal appendices. Those sensitive details should not be included in a publicly posted policy when disclosure would increase security risk.