GUAM CUSTOMS AND QUARANTINE AGENCY

RULES AND REGULATIONS GOVERNING THE AUTOMATED SYSTEM FOR CUSTOMS DATA (ASYCUDA)

CONSOLIDATED AND REVISED PROPOSED RULES

Implementing 5 GCA § 73157 / Public Law 38-109
Administrative Adjudication Law, 5 GCA Chapter 9

Proposed GARR placement and final section numbering are to be confirmed with the Compiler of Laws before formal filing. This draft consolidates the prior CQA draft with the supplemental September 18, 2026 draft material and removes duplicative or unnecessarily technical provisions.

ARTICLE 1 — GENERAL PROVISIONS

§ 101. Authority.
These Rules and Regulations are promulgated by the Director of the Guam Customs and Quarantine Agency pursuant to 5 GCA § 73157, enacted by Public Law 38-109, and the Administrative Adjudication Law, 5 GCA Chapter 9.

§ 102. Purpose.
These Rules govern the effective use, security, integrity, access controls, confidentiality, data retention, and continuity of operations of ASYCUDA and establish the regulatory framework necessary to implement ASYCUDA as CQA's official customs automated system. The Rules are intended to:

- (a) replace fragmented and manual customs processes, to the extent authorized and operationally practicable, with accountable electronic processing;
- (b) support electronic manifests, declarations, assessments, exemptions, collections, releases, audit trails, and related customs transactions;
- (c) strengthen the accuracy, timeliness, traceability, and reliability of customs and revenue information;
- (d) improve interfaces and reconciliation among authorized Government of Guam systems;
- (e) reduce risks associated with unrecorded or unassessed cargo, revenue leakage, fraud, waste, abuse, and weak internal controls;
- (f) protect the confidentiality, integrity, availability, authenticity, and lawful use of ASYCUDA information; and
- (g) facilitate legitimate trade while supporting customs, revenue, law-enforcement, and border-security requirements.

§ 103. Scope and Applicability.
These Rules apply to CQA officers, employees, contractors, consultants, detailees, and authorized representatives; persons authorized or required to transmit or receive information through ASYCUDA; governmental entities granted lawful access to ASYCUDA information; authorized technical, hosting, integration, or support providers; and ASYCUDA modules, interfaces, databases, reports, data exchanges, backups, archives, test or training environments, and associated systems under Agency control.

§ 104. Relationship to Other Law.
These Rules shall be administered consistently with 5 GCA Chapter 73, 5 GCA Chapter 9, applicable tax, records, privacy, procurement, financial-management, customs, trade, and border-security laws, and lawful intergovernmental agreements. Nothing in these Rules creates authority not otherwise granted by law. Controlling law governs in the event of conflict.

ARTICLE 2 — DEFINITIONS

§ 201. Definitions.

(a) “Agency or CQA” means the Guam Customs and Quarantine Agency.

(b) “ASYCUDA” means the Automated System for Customs Data developed, administered, and supplied by the United Nations Conference on Trade and Development, including modules, interfaces, databases, portals, reporting tools, authorized test and training environments, backups, and archives implemented for CQA.

(c) “Authorized User” means a natural person granted unique ASYCUDA credentials by or under the authority of CQA.

(d) “Bill of Lading” means a transportation document or electronic equivalent identifying goods, shipper, consignee, routing, and other shipment information.

(e) “Business Continuity” means the capability to maintain or timely restore essential customs functions following a disruption.

(f) “Carrier” means a person or entity engaged in transporting passengers, cargo, mail, express consignments, vessels, aircraft, or other conveyances into, from, or through Guam.

(g) “Confidential Information” means information protected against unauthorized access, use, or disclosure by law, these Rules, an authorized agreement, or lawful Agency designation, including taxpayer, commercial, personally identifiable, investigative, intelligence, law-enforcement-sensitive, and security information.

(h) “Consolidator” means a person or entity that combines shipments from multiple shippers or house-level shipments into a consolidated shipment for transportation.

(i) “Credential” means a username, password, certificate, token, multifactor-authentication factor, or other approved authentication mechanism.

(j) “Customs Automated System” means an electronic platform or suite of modules used for the receipt and processing of customs declarations, manifests, cargo or passenger data, risk management, valuation, classification, revenue assessment and collection, enforcement actions, and related customs functions.

(k) “Customs Data” means information received, created, processed, transmitted, derived, maintained, or stored in or through ASYCUDA in connection with customs, trade, revenue, passenger, cargo, enforcement, or border-security functions.

(l) “Declarant” means a person legally responsible for submitting a customs declaration, manifest, report, application, or other transaction through ASYCUDA.

(m) “Deconsolidator” means a person or entity that separates a consolidated shipment into house-level or individual shipments.

(n) “Director” means the Director of the Guam Customs and Quarantine Agency, or a lawful designee where delegation is permitted.

(o) “Electronic Record” means information created, generated, submitted, communicated, received, or stored by electronic means.

(p) “External User or Trade User” means an Authorized User who is not acting as CQA personnel and who is authorized to conduct customs or trade transactions or receive information through ASYCUDA.

(q) “Freight Forwarder” means a person or entity arranging transportation, documentation, or related logistics services for cargo on behalf of another person.

(r) “House Bill of Lading” means a bill of lading or equivalent shipment record issued at the individual or house-shipment level by an NVOCC, consolidator, freight forwarder, or other authorized transportation intermediary.

(s) “Incident or Security Incident” means an actual or suspected event jeopardizing the confidentiality, integrity, availability, authenticity, or lawful use of ASYCUDA, its credentials, infrastructure, interfaces, or data.

(t) “Information-Sharing Agreement” means a memorandum of understanding, data-sharing agreement, intergovernmental instrument, or other authorized written agreement governing recurring access to or disclosure of ASYCUDA information.

(u) “Least Privilege” means limiting access rights to the minimum reasonably necessary to perform authorized duties or transactions.

(v) “Manifest” means an air, sea, mail, express-consignment, consolidated, house, master, cargo, passenger, crew, or other transportation manifest required by law or regulation.

(w) “Master Bill of Lading” means a bill of lading or equivalent shipment record issued by the vessel-operating or principal carrier for a consolidated or master shipment.

(x) “Non-Vessel-Operating Common Carrier or NVOCC” means an ocean transportation intermediary that provides common-carrier ocean transportation services without operating the vessel by which the transportation is provided and that may issue its own bills of lading or equivalent shipping documents.

(y) “Privileged Account” means an account possessing administrative, security-management, configuration, database, user-management, or other elevated rights.

(z) “Role-Based Access Control or RBAC” means assignment of system permissions according to authorized duties, legal authority, or business functions.

(27) “System Administrator” means a person specifically authorized by CQA to perform ASYCUDA administration.

(28) “System of Record” means the authoritative Agency source for a defined customs transaction or data element.

(29) “UNCTAD” means the United Nations Conference on Trade and Development.

ARTICLE 3 — ASYCUDA AS THE OFFICIAL CUSTOMS AUTOMATED SYSTEM

§ 301. Official System.
ASYCUDA is the official customs automated system of CQA for customs operations at Guam's ports of entry, including air, sea, mail, and express-consignment facilities, as provided by 5 GCA § 73157.

§ 302. System of Record.
(a) CQA shall designate ASYCUDA as the authoritative system of record for customs transactions and data elements implemented in the system. (b) An electronic transaction accepted and recorded by ASYCUDA constitutes an official Agency record. (c) Where a material conflict exists between ASYCUDA and a legacy or paper record, CQA shall resolve the conflict through an authorized correction, reconciliation, administrative determination, or other lawful process, and shall preserve an audit trail of the resolution.

§ 303. System Configuration.
CQA shall configure and operate ASYCUDA, to the maximum extent practicable and consistent with law, to receive, process, validate, retain, assess, account for, reconcile, and report customs and revenue

transactions electronically and to preserve Government of Guam ownership, control, and timely access to Customs Data regardless of hosting or service arrangement.

§ 304. Phased Electronic Processing.
The Director may establish phased implementation schedules identifying declarations, manifests, permits, supporting documents, assessments, payments, releases, applications, reports, and other transactions to be processed electronically. Implementation may be phased by port, transportation mode, carrier class, cargo type, module, transaction type, or user category.

§ 305. Published Filing Requirements.
Filing deadlines, data specifications, and implementation instructions shall be based on existing statutory or regulatory authority and may be published through CQA notices, technical specifications, or user instructions. A technical instruction shall not create a substantive public obligation beyond applicable law and duly promulgated regulations.

ARTICLE 4 — ELECTRONIC MANIFESTS, DECLARATIONS, AND RECORDS

§ 401. Electronic Filing.
Except where otherwise required by law or authorized by CQA because of transition, outage, emergency, or other documented circumstances, transactions designated for electronic processing shall be submitted through ASYCUDA.

§ 402. Accuracy, Completeness, and Timeliness.
A person submitting information through ASYCUDA shall provide complete, accurate, and timely information; exercise reasonable care; use only an authorized account; provide or retain required supporting documentation; and promptly correct discovered material errors through authorized procedures.

§ 403. Electronic Attribution.
Use of an authenticated credential constitutes evidence that a transaction was submitted under authority of the registered account holder, subject to evidence of credential compromise, unauthorized use, system error, or other circumstances established to CQA. This section does not alter any requirement for a signature, certification, or evidentiary showing imposed by other law.

§ 404. Advance Cargo and Conveyance Information.
ASYCUDA shall, where configured by CQA and where authorized or required by law, receive advance manifest, airway bill, bill of lading, passenger, crew, conveyance, and related cargo information.

§ 405. Master and House Shipment Data.
Where consolidated cargo is reported, CQA may require electronic linkage between master-level and house-level shipment information sufficient to identify the carrier, NVOCC, consolidator or deconsolidator, shipper, consignee, cargo description, routing, and release status as authorized by law.

§ 406. Amendment and Cancellation.
(a) An electronic record may be amended or cancelled only through an authorized system function or documented administrative process. (b) ASYCUDA shall preserve, to the extent technically practicable, the original information, revised information, date and time, identity of the user or approving official, and reason for the action. (c) No amendment or cancellation may be used to conceal evidence or obstruct an audit, assessment, investigation, or enforcement action.

§ 407. Prohibited Submissions.
No person may knowingly submit materially false or misleading information, manipulate data to evade a lawful duty or enforcement action, conceal or materially misdescribe cargo, alter another person's submission without authority, or intentionally circumvent an ASYCUDA validation or security control.

ARTICLE 5 — USER REGISTRATION, ACCESS CONTROL, AND ACCOUNT ADMINISTRATION

§ 501. Registration and Authorization.
No person may access ASYCUDA unless registered or otherwise authorized by CQA. External registration does not confer a professional license, customs-representative authority, or other legal status that requires independent statutory authorization.

§ 502. Identity and Organizational Information.
CQA may require information reasonably necessary to verify identity, organizational affiliation, legal authority to conduct the requested transactions, contact information, and the individual users for whom access is requested.

§ 503. Role-Based Access and Least Privilege.
Access shall be based on documented job function, legal authority, operational necessity, least privilege, and separation of incompatible duties where reasonably practicable. CQA shall maintain a controlled role catalog or equivalent access matrix.

§ 504. Unique Accounts and Service Accounts.
Each Authorized User shall use an individually attributable account. Shared user credentials are prohibited. Technical service accounts may be permitted only when specifically authorized, controlled, attributable to a responsible owner, and subject to enhanced review.

§ 505. Authentication.
CQA shall establish risk-appropriate authentication requirements and may require multifactor authentication, password controls, digital certificates, device authentication, network restrictions, or other safeguards consistent with current Government of Guam security standards.

§ 506. Privileged Access.
Privileged access shall be limited to named persons with a documented need, separately identifiable where practicable, subject to enhanced logging and review, and promptly modified or revoked when no longer necessary. Vendor or UNCTAD privileged access shall be limited to authorized support activities and governed by applicable agreements and Agency controls.

§ 507. Account Lifecycle.
CQA shall maintain documented procedures for account request, approval, provisioning, modification, periodic recertification, suspension, and termination. Access shall be promptly modified or disabled when a user separates, changes duties, loses required authorization, presents a material security risk, or no longer has a legitimate need for access.

§ 508. External User Responsibilities.
An organization receiving external access shall promptly notify CQA when an authorized employee or representative separates, changes duties, no longer requires access, or when credentials may have been compromised.

ARTICLE 6 — USER SECURITY AND ACCEPTABLE USE

§ 601. Credential Protection.
Users shall safeguard credentials and authentication factors and shall not share, disclose, transfer, or permit another person to use assigned credentials.

§ 602. Authorized Use.
ASYCUDA shall be used only for official governmental duties or authorized customs and trade transactions. Users shall not access unrelated records for personal, commercial, political, curiosity-driven, or other unauthorized purposes.

§ 603. Prohibited Technical Activity.
No user shall knowingly disable or circumvent a security control; introduce malicious or unauthorized code; conduct unauthorized probing, scraping, bulk extraction, or automated activity; connect unapproved systems in a manner that creates material risk; or interfere with ASYCUDA availability or integrity.

§ 604. Compromise Reporting.
A user or organization shall report suspected credential compromise, unauthorized access, or material misuse to CQA without unreasonable delay and shall cooperate with protective measures, investigation, credential reset, and account review.

§ 605. Monitoring Notice.
System activity may be logged, monitored, reviewed, and audited for security, compliance, customs enforcement, revenue assurance, system administration, and other lawful governmental purposes.

ARTICLE 7 — INFORMATION SECURITY AND CYBERSECURITY

§ 701. Information Security Program.
CQA shall maintain a written ASYCUDA information-security program appropriate to system risk and consistent with applicable Government of Guam requirements and generally accepted governmental cybersecurity practices.

§ 702. Risk Assessment.
CQA shall periodically assess material risks to ASYCUDA and reassess risk following significant changes to system architecture, hosting, interfaces, or threat conditions. Material risks and corrective actions shall be documented and tracked.

§ 703. Encryption and Secure Transmission.
CQA shall use appropriate safeguards for Customs Data in transit and at rest based on sensitivity, operational requirements, and applicable law or government security standards.

§ 704. Vulnerability, Patch, and Configuration Management.
CQA shall maintain documented procedures for vulnerability management, security updates, configuration control, and remediation based on severity and risk. Specific technical timelines may be established in controlled security standards or plans.

§ 705. Change Management.
Material changes to production configuration, code, interfaces, tariff or reference data, or security settings shall be authorized, tested where practicable, documented, and subject to rollback or recovery procedures. Emergency changes shall be documented and reviewed after implementation.

§ 706. Test and Training Environments.
Production Confidential Information shall not be used in test, development, or training environments unless appropriately protected, masked, de-identified, or specifically authorized under controls equivalent to the sensitivity of the information.

§ 707. Audit Logging.
ASYCUDA shall maintain logs sufficient to support accountability for authentication, material customs transactions, amendments, assessments, exemptions, waivers, releases, user and role changes, reference-data changes, privileged activity, and significant exports or extractions. Logs shall be protected against unauthorized alteration and reviewed according to risk.

§ 708. Third-Party Security.
Agreements with UNCTAD, hosting providers, integrators, and technical-service providers shall address, as applicable, security responsibilities, authorized access, data locations, subcontracting, incident notification, audit or assurance rights, continuity, data return, and secure disposition at termination.

ARTICLE 8 — DATA INTEGRITY, REVENUE CONTROLS, AND AUDITABILITY

§ 801. Validation and Integrity Controls.
CQA shall configure automated or procedural controls, as appropriate, to validate required data fields, code sets, tariff classifications, valuation information, exchange rates, exemption information, and calculations used in customs and revenue processing.

§ 802. Separation of Duties.
CQA shall separate incompatible high-risk functions where reasonably practicable, including assessment and waiver, amendment and release approval, external-user administration and filing, and audit-log administration. Where staffing or technical constraints prevent full segregation, CQA shall document and apply compensating controls.

§ 803. Overrides and Exceptional Corrections.
Material overrides of system controls and database-level corrections shall require documented authorization, an identified reason, individually attributable execution, and an audit trail. Direct alteration or deletion of official transaction history outside authorized procedures is prohibited.

§ 804. Revenue Traceability.
ASYCUDA shall support transaction-level traceability, to the extent practicable, among declarations, assessments, exemptions, waivers, payments, refunds, adjustments, deposits, and related accounting records.

§ 805. Revenue Reconciliation.
CQA shall maintain documented reconciliation procedures between ASYCUDA revenue information and authorized Government of Guam collection, treasury, accounting, or financial-management records. Material unreconciled differences shall be investigated, documented, escalated according to risk, and resolved.

§ 806. Exemption Controls.
Claims of exemption, exclusion, threshold, waiver, or other preferential treatment processed through ASYCUDA shall be supported by the information or documentation required by law and shall be subject to appropriate validation, supervisory review, audit, or exception controls.

§ 807. Reference Data.
Tariff schedules, rates, exemption codes, exchange rates, trader registries, and other controlled reference data shall be maintained through authorized change procedures with effective dates and sufficient historical information to reproduce prior transactions.

§ 808. Data Quality Monitoring.
CQA shall monitor data-quality indicators such as rejected submissions, amendments, incomplete manifests, unresolved exceptions, late filings, and reconciliation discrepancies and may use such information for training, compliance, system improvement, and enforcement authorized by law.

ARTICLE 9 — CONFIDENTIALITY, DATA GOVERNANCE, AND INFORMATION USE

§ 901. Protected Information.
Customs Data shall be classified and protected according to applicable law and sensitivity. Protected categories may include taxpayer information; confidential commercial or financial information; personally identifiable information; law-enforcement-sensitive, investigative, intelligence, and targeting information; credentials; and system-security information.

§ 902. Need-to-Know and Purpose Limitation.
No person shall access, use, or disclose Confidential Information except as necessary for an authorized duty or transaction and for a lawful purpose.

§ 903. Permitted Disclosures.
Confidential Information may be disclosed only as authorized by law, to an authorized governmental recipient under Article 11, to the person who submitted the information or an authorized representative where permitted, pursuant to lawful compulsory process, to an authorized auditor subject to applicable confidentiality requirements, or as otherwise expressly authorized by law.

§ 904. Public Records Requests.
Requests for ASYCUDA information under Guam public-records law shall be processed by the appropriate Agency records official. CQA shall apply statutory exemptions and redactions as required by law. These Rules do not create an independent exemption from disclosure.

§ 905. Aggregate and Statistical Information.
CQA may publish aggregate or statistical trade information when release is lawful and reasonably designed to avoid disclosure of protected transaction-level or personally identifiable information.

§ 906. Data Governance.
CQA shall maintain a Data Governance Policy addressing data ownership, stewardship, classification, quality, metadata, authoritative sources, access, sharing, retention, legal holds, disposition, and periodic review.

ARTICLE 10 — DATA OWNERSHIP, RETENTION, AND DISPOSITION

§ 1001. Government Ownership and Control.
Consistent with 5 GCA § 73157(f), the Government of Guam shall retain ownership, control, and timely access to customs and revenue-related data processed through ASYCUDA regardless of hosting, licensing, support, or service arrangement.

§ 1002. Data Portability and Continuity of Access.
CQA shall maintain the practical ability to obtain Customs Data in a usable, documented, and reasonably portable format sufficient to support continuity, audit, migration, and lawful records obligations. Applicable agreements shall not permit a provider to withhold Government of Guam data because of a contract or fee dispute except as otherwise required by law.

§ 1003. Retention Schedule.
CQA shall maintain an approved records-retention schedule for ASYCUDA records consistent with applicable Guam records law, tax and audit requirements, enforcement needs, litigation holds, and other controlling retention requirements. Specific retention periods may be established through an approved records schedule or other lawful instrument rather than fixed in these Rules unless required by law.

§ 1004. Data Minimization.
CQA shall not knowingly collect or retain personally identifiable or other sensitive data beyond an authorized operational, revenue, enforcement, audit, records, or legal need.

§ 1005. Legal Holds.
CQA shall suspend ordinary disposition of records subject to actual or reasonably anticipated litigation, audit, investigation, administrative proceeding, public-records dispute, or other lawful hold.

§ 1006. Secure Disposition.
Records eligible for destruction shall be disposed of only through authorized records procedures and in a manner reasonably designed to prevent unauthorized reconstruction or disclosure. Disposition shall be documented.

ARTICLE 11 — INTEROPERABILITY, INFORMATION SHARING, AND INTERAGENCY COOPERATION

§ 1101. Department of Revenue and Taxation Interface.
Consistent with 5 GCA § 73157(f), CQA shall pursue and maintain, to the maximum extent practicable and as authorized by law, electronic interfaces with the Department of Revenue and Taxation supporting taxpayer or account validation, assessment, exemption, collection, reconciliation, reporting, and enforcement functions.

§ 1102. Government Financial and Revenue Systems.
CQA shall pursue interfaces with authorized government-wide financial or revenue-management systems to improve the recording, classification, reconciliation, and reporting of customs receipts and related revenue and to reduce unnecessary manual re-entry.

§ 1103. Other Government Interfaces.
CQA may integrate ASYCUDA with other authorized Government of Guam systems where there is a lawful customs, revenue, trade, logistics, statistical, enforcement, or border-security purpose.

§ 1104. Information-Sharing Agreements.
Before providing recurring system access or a recurring data feed to another governmental entity, CQA shall document the legal authority, purpose, data elements, permitted uses, safeguards, access controls, retention expectations, incident-notification responsibilities, audit or accountability provisions, and termination conditions through an Information-Sharing Agreement or other appropriate written instrument.

§ 1105. Federal, Regional, and International Cooperation.
Subject to applicable local and federal law and confidentiality requirements, CQA may use ASYCUDA to support lawful information exchange and cooperation with federal authorities and regional or international customs entities for customs, revenue, law enforcement, border security, trade facilitation, risk management, or related governmental purposes authorized by 5 GCA § 73157(h).

§ 1106. No Automatic Disclosure.
No disclosure is authorized solely because ASYCUDA is an international customs platform or because another entity requests access. Each disclosure or recurring exchange must have independent legal authority and appropriate safeguards.

§ 1107. Standards and Interoperability.
In configuring ASYCUDA, CQA may use internationally recognized customs, trade, data, and interoperability standards where consistent with Guam law and operational requirements. Reference to an external standard does not independently impose a legal obligation on the public unless adopted or required through applicable law or these Rules.

ARTICLE 12 — CONTINUITY OF OPERATIONS AND DISASTER RECOVERY

§ 1201. Continuity and Disaster-Recovery Plan.
CQA shall maintain a written ASYCUDA Continuity of Operations and Disaster Recovery Plan addressing material disruptions, including loss of facilities, hosting, power, telecommunications, vendor support, or system availability; typhoon or other natural disaster; and cybersecurity incidents.

§ 1202. Critical Functions and Recovery Priorities.
The Plan shall identify critical customs and revenue functions, dependencies, recovery priorities, responsible personnel, alternate procedures, communications, and recovery objectives based on a documented business-impact analysis.

§ 1203. Backups and Restoration.
CQA shall maintain protected backups appropriate to system risk and shall periodically test restoration and integrity. Specific backup frequencies, recovery-time objectives, and recovery-point objectives shall be maintained in controlled technical plans or service agreements and reviewed periodically.

§ 1204. Alternative Processing.
When ASYCUDA is unavailable, the Director may activate controlled contingency procedures, including paper or alternate electronic processing, delayed transmission, emergency cargo-release procedures, provisional revenue procedures, or other temporary controls consistent with law.

§ 1205. Contingency Accountability.
Contingency transactions shall be uniquely identified and sufficiently documented to preserve accountability, custody, assessment, collection, exemption, hold, examination, and release information.

§ 1206. Post-Restoration Reconciliation.
Transactions processed during an outage or degraded operation shall be entered into or reconciled with ASYCUDA as soon as reasonably practicable after restoration, and material exceptions shall be reviewed and resolved.

§ 1207. Exercises.
CQA shall periodically exercise continuity and disaster-recovery procedures with relevant system and governmental partners as appropriate and shall document corrective actions.

ARTICLE 13 — CYBERSECURITY INCIDENT RESPONSE

§ 1301. Incident Response Plan.
CQA shall maintain a written incident-response plan addressing preparation, detection, reporting, triage, containment, eradication, recovery, evidence preservation, notification, documentation, and post-incident review.

§ 1302. Protective Measures.
Upon reasonable evidence of compromise or material risk, CQA may suspend an account, terminate a session, block a device or network connection, restrict system functionality, preserve logs, isolate affected systems, or take other reasonable protective measures consistent with law.

§ 1303. Incident Reporting.
CQA personnel and Authorized Users shall report suspected material security incidents through designated channels without unreasonable delay.

§ 1304. Notification.
CQA shall make incident or breach notifications to affected governmental partners, users, individuals, oversight entities, or law-enforcement authorities when required by applicable law, agreement, or documented incident-response procedure. Notification may be delayed where lawfully necessary to protect an investigation or system recovery.

§ 1305. Post-Incident Review.
Significant incidents shall be documented and reviewed for cause, impact, affected information, corrective action, control deficiencies, and measures necessary to reduce recurrence.

ARTICLE 14 — SYSTEM GOVERNANCE, ADMINISTRATION, AND CHANGE CONTROL

§ 1401. Director's Responsibility.
The Director has executive responsibility for the lawful governance and administration of ASYCUDA and may designate system administrators, data stewards, security officials, records officials, and other responsible personnel.

§ 1402. Separation of Security and Administration.
CQA shall structure system-administration and security-oversight responsibilities to provide independent review of privileged access and material security actions to the extent practicable.

§ 1403. ASYCUDA Governance Committee.
The Director may establish an ASYCUDA Governance Committee to advise on configuration, deployment, interfaces, data governance, cybersecurity, access controls, revenue controls, continuity, training, performance, and change priorities. Membership may include appropriate CQA functions and representatives of other Government of Guam entities when their participation is relevant.

§ 1404. Performance and Control Review.
CQA shall periodically review system availability, transaction volumes, revenue and reconciliation information, data-quality indicators, interface performance, significant security findings, continuity readiness, and material exceptions or overrides.

§ 1405. Technical Documentation.
CQA shall maintain sufficient system, configuration, interface, security, operational, and change documentation to support administration, audit, continuity, and transfer of responsibilities.

ARTICLE 15 — TRAINING, EXTERNAL USERS, AND USER CONDITIONS

§ 1501. Training.
CQA may require role-appropriate ASYCUDA training before granting or maintaining access. Training may address system operation, customs procedures, data quality, cybersecurity, confidentiality, records management, incident reporting, revenue controls, and user-specific responsibilities.

§ 1502. Competency.
The Director may require designated classes of users to demonstrate competency or complete refresher training when reasonably necessary for safe and accurate system use.

§ 1503. External User Terms and Conditions.
CQA shall maintain External User Terms and Conditions consistent with these Rules. Acceptance of those terms may be required as a condition of external access, but the terms shall not create substantive obligations beyond applicable law and these Rules.

§ 1504. Technical Support and User Guidance.
CQA may publish user guides, help materials, technical specifications, training materials, frequently asked questions, and implementation notices to support compliance and system use.

ARTICLE 16 — AUDIT, COMPLIANCE, AND CORRECTIVE MEASURES

§ 1601. Compliance Reviews.
CQA may review and audit ASYCUDA access, transactions, system activity, and supporting records to determine compliance with applicable law, these Rules, and lawful conditions of access.

§ 1602. User Cooperation.
Authorized Users shall reasonably cooperate with lawful Agency inquiries concerning transactions conducted under their credentials, data errors, suspected misuse, security incidents, and compliance reviews.

§ 1603. Preservation of Evidence.
No person shall knowingly alter, conceal, or destroy information reasonably believed to be subject to a legal hold or material to an audit, investigation, administrative proceeding, civil proceeding, or criminal proceeding.

§ 1604. Administrative Measures.
As authorized by law, violation of these Rules may result in warning, mandatory retraining, modification of privileges, temporary suspension or termination of ASYCUDA access, referral for personnel or administrative action, customs enforcement, referral to another governmental agency, or another independently authorized remedy.

§ 1605. Summary Protective Suspension.
CQA may immediately suspend or restrict access where continued access presents a reasonable and material threat to ASYCUDA security, integrity, availability, revenue protection, or border security. CQA shall provide any notice, opportunity to respond, hearing, or other process required by applicable law.

§ 1606. No Unauthorized Penalties.
These Rules do not create a monetary penalty, criminal offense, professional licensing sanction, forfeiture, or other substantive sanction not otherwise authorized by statute.

ARTICLE 17 — TRANSITION AND IMPLEMENTATION

§ 1701. Phased Migration.
The Director may establish a phased migration from legacy customs processes and systems to ASYCUDA.

§ 1702. Parallel Operations.
During transition, CQA may temporarily operate ASYCUDA and legacy processes concurrently to validate data, assessments, revenue, interfaces, cargo-release processes, enforcement controls, and operational readiness.

§ 1703. Historical Data.
CQA may migrate historical customs records to ASYCUDA when technically feasible and operationally appropriate, subject to data-quality, confidentiality, security, and records requirements.

§ 1704. Termination of Legacy Processes.
Upon a documented determination that an ASYCUDA function is sufficiently operational and reliable, the Director may discontinue a superseded legacy process, subject to applicable records, continuity, and legal requirements.

§ 1705. Implementation Plan.
CQA shall maintain the implementation plan required by Public Law 38-109, including projected phased deployment, major milestones, training, integration with the Department of Revenue and Taxation and other relevant agencies, anticipated budget and funding sources, and measures addressing previously identified deficiencies in customs processing, assessment, collection, and internal controls.

ARTICLE 18 — IMPLEMENTING PROCEDURES, CONSTRUCTION, AND EFFECTIVE DATE

§ 1801. Companion Policies and Procedures.
The Director may issue policies, standard operating procedures, security standards, technical bulletins, data specifications, implementation schedules, user instructions, and administrative directives necessary to implement these Rules, including an ASYCUDA Data Governance Policy; Access Control and User Administration SOP; Cybersecurity and Incident Response Plan; Continuity of Operations/Disaster Recovery Plan; Information Sharing Agreement Template; and External User Terms and Conditions.

§ 1802. Limitation on Implementing Instruments.
A policy, SOP, technical standard, user condition, or other implementing instrument shall be consistent with applicable law and these Rules and shall not enlarge or diminish a substantive public right or obligation established by statute or duly promulgated regulation.

§ 1803. Sensitive Technical and Enforcement Information.
CQA shall protect technical, cybersecurity, enforcement, targeting, credential, architecture, and other sensitive information from public disclosure to the extent authorized or required by law. Nothing in this section creates an independent public-records exemption.

§ 1804. Waiver of Procedural Requirements.
Where authorized by law and not inconsistent with a mandatory statutory requirement, the Director may grant a written, time-limited exception to an Agency-established procedural or technical requirement upon a documented finding of operational necessity and adequate compensating controls. This section does not authorize waiver of statutory duties, confidentiality requirements, or Government of Guam ownership and control of Customs Data.

§ 1805. Construction.
These Rules shall be liberally construed to implement 5 GCA § 73157 while preserving the limits of CQA's statutory authority.

§ 1806. Severability.
If any provision of these Rules or its application to a person or circumstance is held invalid, the remainder shall not be affected to the extent it can be given effect independently.

§ 1807. Effective Date.
These Rules shall become effective only upon completion of the requirements of the Administrative Adjudication Law, 5 GCA Chapter 9, and other applicable law.

APPENDIX — CONSOLIDATION AND DRAFTING NOTES

This appendix is for CQA/Attorney General review and may be removed from the version formally promulgated as regulations.

A. Principal Redundancies Removed

- User registration, account lifecycle, credential responsibility, external-user access, and organizational notification requirements were consolidated into Articles 5, 6, and 15 rather than repeated across separate access, trade-user, and enforcement articles.
- Cybersecurity program requirements, incident response, breach notification, and protective actions were separated into Articles 7 and 13, while duplicative incident language was removed.
- Data integrity, overrides, reference data, exemption controls, revenue traceability, and reconciliation were consolidated into Article 8.
- Confidentiality, purpose limitation, public-records handling, statistical release, and data governance were consolidated into Article 9.
- Data ownership, portability, retention, legal hold, and disposition were consolidated into Article 10.
- DRT interfaces, financial-system interfaces, data-sharing agreements, federal/regional cooperation, and interoperability standards were consolidated into Article 11.
- Continuity, backups, alternative processing, outage accountability, and post-restoration reconciliation were consolidated into Article 12.
- System governance, administrator responsibilities, governance committee, performance review, and technical documentation were consolidated into Article 14.
- Enforcement provisions were narrowed and consolidated in Article 16 to avoid creating sanctions not independently authorized by statute.

B. Useful Supplemental Provisions Incorporated

- Master/house bill relationships and NVOCC/consolidator terminology for electronic manifest design.
- Stronger transaction-level revenue traceability, exemption documentation, reconciliation, and reference-data controls responsive to the Legislature's findings.
- Controlled privileged access, service accounts, audit logging, change management, test/training environment controls, and third-party security requirements.
- Data portability and continuity-of-access requirements supporting Government of Guam ownership and control.
- Business-impact-based continuity planning, contingency accountability, restoration testing, and post-outage reconciliation.
- Information-sharing agreements with purpose limitation, security, retention, incident, accountability, and termination terms.
- Implementation-plan language tied directly to Public Law 38-109's initial reporting requirements.

C. Provisions Deliberately Not Carried Forward as Fixed Regulatory Mandates

- Fixed password rules, inactivity timeouts, patch deadlines, backup frequencies, recovery-time/recovery-point objectives, and penetration-test cycles. These are better maintained in controlled security/COOP standards that can evolve with technology and demonstrated capability.
- Fixed record-retention periods. Final periods should be aligned with Guam records schedules, tax/audit requirements, and legal holds before adoption.
- A categorical rule that ASYCUDA automatically overrides every paper or legacy record. The revised draft instead requires documented reconciliation and correction.
- A categorical statement that every authenticated electronic record has the same legal effect as a signed paper record in all proceedings. The revised draft preserves attribution without attempting to alter independent signature or evidence law.

- Automatic denial or revocation of system access for unpaid liabilities or other conditions not clearly established as independent statutory prerequisites.
- Mandatory external standards as binding law merely by reference. The revised draft permits use of recognized standards without improperly delegating lawmaking to an external body.
- Mandatory source-code escrow, fixed vendor attestations, or other contractual terms not expressly required by Public Law 38-109. The revised rules preserve data ownership, portability, security, and continuity while leaving negotiated technical terms to the authorized UNCTAD agreement.
- New monetary penalties, licensing regimes, criminal offenses, or forfeitures not independently authorized by statute.

D. Primary Authorities Reviewed

Public Law 38-109 (Bill No. 234-38 (COR), signed April 8, 2026), including its legislative findings, 5 GCA § 73157, and the implementation/reporting provisions; and 5 GCA Chapter 9, Administrative Adjudication Law. Final legal sufficiency, GARR placement, section numbering, retention schedules, and compatibility with existing CQA regulations should be confirmed before formal publication.