GOVERNMENT OF JAMAICA

ELECTRONIC SIGNATURES AND ELECTRONICALLY SIGNED RECORDS POLICY

Ministry of Finance and the Public Service

September 1, 2026

Contents

1. Policy Statement

This Electronic Signature and Electronically Signed Records Policy establishes the Government of Jamaica's (GOJ) standard governing the lawful, secure, and auditable use of electronic signatures and electronically signed records in the conduct of official business by way of Cabinet Decision #23/26.

In accordance with the Electronic Transactions Act (ETA), a signature or record shall not be denied legal effect solely because it is in electronic form.

All Ministries, Departments and Agencies (MDAs) and public bodies that adopt electronic signature methods shall comply with this Policy.

Nothing in this Policy prevents the continued use of wet-ink signatures where specifically required by law.

2. Legal and Policy Context

The GOJ continues to advance the use of digital technologies to improve efficiency, accountability, and continuity in the conduct of official business. The use of electronic signatures and electronic records is a key enabler of this objective.

The use of electronic signatures and electronic records in Jamaica is supported by existing legislation, specifically the ETA.

The ETA provides legal recognition for electronic records and electronic signatures and confirms that a signature or record shall not be denied legal effect solely because it is in electronic form. The Act also provides for the use of digital signatures and establishes a framework for certification services.

Regulations 76 and 77 of the Financial Management Regulations, 2011, recognise electronic records in the conduct of public financial management. Other legislation governing public administration, procurement, records management, and data protection also contemplates the use of electronic systems.

Consequently, the Act and Regulations confirm that electronic signatures are legally valid and enforceable under Jamaican law.

This Policy establishes principles, risk-based assurance expectations, and minimum control requirements. Detailed cryptographic standards, certificate architecture, and system configuration requirements should be addressed separately through technical standards or implementation guidance issued by the Information and Communications Technology (ICT) Authority or other competent authorities.

This Policy should be read in conjunction with applicable laws, regulations, and instructions governing public administration, financial management, records management, and data protection.

3. Purpose

This Policy provides a structured and consistent framework for the use of electronic signatures and for ensuring the integrity and management of electronically signed records in the conduct of official Government business. It is intended to:

- support business continuity and improve efficiency in operational transactions that were previously conducted using wet signatures and paper documents;
- promote trust and enhance security, authenticity, integrity, and accountability in electronic transactions and electronically signed records;
- provide clarity to public officers regarding the lawful and appropriate use of electronic signatures;
- promote consistent practices across Ministries, Departments, Agencies, and public bodies; and
- ensure that electronic signature practices align with applicable legislative and regulatory requirements.

This Policy establishes a risk-based approach to the selection and implementation of electronic signature methods appropriate to the nature and impact of the transaction.

The purpose of this Policy is not to create that legal validity, but to provide practical guidance to ensure that electronic signatures are implemented in a secure, consistent, and auditable manner across Government.

4. Scope and Applicability

This Policy applies to the use of electronic signatures and to electronic records that are signed or approved electronically in the conduct of official Government business, across document execution platforms, enterprise workflow systems, and digital record repositories. This Policy applies to MDAs and public bodies that adopt electronic signature methods for official transactions. Official business includes, *but is not limited* to:

- internal approvals and authorisations;
- memoranda and official correspondence requiring signature;
- procurement processes and recommendations;
- contracts and agreements;
- payment vouchers, invoices, and other financial management records;
- human resource actions; and
- regulatory or statutory instruments.

Where electronic signatures are adopted in any of the above contexts, their use should align with the principles and minimum standards set out in this Policy.

Where an electronic signature meets the applicable risk-based assurance requirements and is not prohibited by statute, public entities shall not require a wet-ink signature solely on the basis that the document is in electronic form. Properly implemented electronic signatures must provide strong authentication, integrity protection, and auditability

5. Definitions

Where a term is defined in the Electronic Transactions Act, the statutory meaning applies. For ease of reference, key terms used in this Policy are set out below.

TERM	MEANING
Assurance Level	The level of confidence that an electronic signature method provides regarding the identity of the signatory, the integrity of the record, and the reliability of the evidence supporting the signing action.
Audit Trail	A secure record of system events capturing user identity, date and time of action, and details of the transaction.
Authentication	The process of verifying the identity of a user before granting access or authority to sign or approve a record.
Certificate-Based Signature	A digital signature generated using a cryptographic key pair, where the signer's public key is bound to their identify through a digital certificate issued by a recognised certification authority under an applicable trust framework.
Credential	A means used to authenticate identity or authority within a system, including a password, token, biometric factor, or digital certificate.
Digital Certificate	An electronic credential that binds a public key to an identified individual or entity for purposes of verifying digital signatures.
Digital Signature	A type of electronic signature that uses cryptographic methods to create a secure and verifiable link between the signatory and the electronic record, enabling verification of the signer's identity and the integrity of the record.
Electronic Record	Any information and documentation created, generated, received, stored, or communicated by electronic means and capable of being retained and reproduced.
Electronic Signature	Any electronic sound, symbol, process or method attached to or logically associated with a record and executed or adopted by a person with the intention of signing or approving that record.
Image-Based Signature	A visual representation of a handwritten signature inserted into an electronic document, without cryptographic protection or independent certificate validation.
Multi-Factor Authentication (MFA)	An authentication method requiring two or more independent credentials, such as something the user knows, something the user has, or something the user is, to verify identity.
Official Business	Any transaction, communication, approval, or action undertaken in the course of Government functions or service delivery.

TERM	MEANING
Self-Signed Certificate	A digital certificate created and signed by the user or organisation without validation by an independent certification authority.
Signatory	A signatory is a person who applies, adopts, or authorises an electronic signature or approval to a record, with the intention of signing or approving its contents, and whose identity can be reliably associated with that act.
System-Generated Signature	An electronic signature automatically applied by an information system in accordance with predefined rules and controls, without direct manual action at the time of application.
Trust Framework	The set of policies and arrangements that determine how digital certificates and electronic signatures are issued, recognised, and relied upon.
Workflow-Based Approval	An approval executed within an authenticated information system where the identity of the approver, date and time of approval, transaction context, and an audit trail are recorded.

6. Principles Governing the Use of Electronic Signatures

The use of electronic signatures and electronic records must be guided by the following principles:

- **Legality**: Electronic signatures must comply with applicable legislative and regulatory requirements and must not be denied legal effect solely because they are in electronic form.
- **Authenticity**: The identity of the signatory must be verifiable and capable of being established through appropriate authentication mechanisms.
- **Integrity**: Electronic records must be protected against unauthorised alteration or modification. Any alteration or modification after signing must be detectable.
- **Accountability**: Signing actions must be traceable to an identifiable individual, or authorised system process, and reliable audit trails must be maintained.
- **Proportionality**: The level of assurance applied to an electronic signature must be appropriate to the risk and legal significance of the transaction.
- **Technology Neutrality**: This Policy does not mandate specific vendors or products. Solutions should meet control expectations regardless of technology platform.
- **Interoperability**: Electronic signature solutions should support verification and validation across Government entities, consistent with ICT standards provided by the ICT Authority.

7. Governance and Accountability

The Head of Entity or designated Accountable Officer is responsible for ensuring that electronic signature practices within the entity comply with this Policy and with applicable governance frameworks.

MDAs adopting electronic signatures must:

- designate responsibility for implementation and ongoing oversight;

- formally document the risk classification of transaction categories eligible for electronic signing;
- ensure that electronic signature controls are incorporated into internal control systems;
- ensure that electronically signed records are managed in accordance with applicable records management requirements;
- monitor compliance with this Policy; and
- ensure that suspected compromise of signing credentials is managed in accordance with established ICT security procedures.

Electronic signature practices must be aligned with existing financial management, procurement, ICT security, and administrative governance frameworks.

8. Use of Electronic Signatures

Electronic signatures may be used for a wide range of official business, provided that:

- The identity of the signatory can be established.
- The signatory has the intention to sign or approve the record.
- The signature is logically associated with the electronic record; and
- Appropriate controls exist to ensure integrity and auditability.

MDAs must ensure that the type of electronic signature selected is proportionate to the risk and legal significance of the transaction.
Where electronic signatures are used, electronically signed records must be retained in a manner that preserves their integrity and reliability for evidentiary and audit purposes.

9. Signature Risk Categories and Assurance Levels

MDAs are required to classify transactions based on risk and document that classification. Risk assessment should consider:

- financial exposure;
- legal consequences;
- regulatory impact;
- reputational implications; and
- operational significance.

The level of assurance applied to an electronic signature must correspond to the assessed risk of the transaction.

9.1 Risk Categories

Risk Category	Examples	Minimum Assurance
Low Risk	Routine internal acknowledgements, administrative memos	Secure electronic signature with a record confirming who signed the document and when it was signed
Moderate Risk	Human Resource approvals, procurement recommendations, financial authorisations	Digital signature with strong authentication (e.g. MFA)
High Risk	Contracts, statutory instruments, high-impact regulatory decisions, transactions with significant financial or legal consequences	Certificate-based digital signature recognised under the statutory certification framework

9.2 Image-Based Signatures

Image-based representations of signatures may be accepted for low or moderate-risk transactions where:

- the identity of the sender can be reasonably established through official communication systems; and
- the transaction does not involve high-risk obligations.

Image-based signatures do not provide cryptographic protection and should not be relied upon where higher levels of assurance are required.

The use of an individual's signature should not be delegated, as such no image-based signature may be used without the owner of the signature using same to sign the document.

9.3 Self-Signed Certificates

Self-signed certificates may be used for low or moderate-risk internal transactions where identity and credential issuance are controlled within the organisation.

Self-signed certificates must not be used for high-risk transactions

Self-signed certificates created by individual users using commercial software tools are not equivalent to certificates issued under a recognised certification framework.

Organisationally issued internal certificates may provide higher assurance than individual self-created certificates but remain distinct from certificate-based signatures recognised under the framework of the ETA.

Where self-signed certificates are used, MDAs should ensure that internal controls provide appropriate assurance regarding identity and integrity.

10. Workflow-Based and System-Generated Signatures

Government operations increasingly rely on enterprise information systems that implement structured approval workflows. Electronic approvals executed within authenticated Government information systems constitute valid electronic signatures where:

- user identity is authenticated;
- the approval action is logically associated with the relevant transaction or record;
- the system records the approval action, timestamp, and transaction context; and
- a secure audit trail is maintained.

System-generated signatures applied automatically by approved Government systems may constitute valid electronic signatures where:

- the automated application of the signature is governed by formally approved rules;
- the triggering conditions for signature application are documented; and
- system logs capture the relevant transaction events and responsible authority.

Workflow-based and system-generated approvals within approved Government enterprise systems may be treated as authoritative electronic signatures and may constitute original records for evidentiary and audit purposes, provided they meet the authenticity, integrity, and retention requirements above.

Where system-based controls provide equivalent or greater assurance than document-based signing methods, duplicative wet-ink or document-level electronic signatures should not be required.

11. Minimum Control Requirements for Electronic Signature Use

MDAs adopting electronic signature methods must implement controls sufficient to ensure the authenticity, integrity, accountability, and reliability of electronically signed records.

11.1 Identity and Authentication Controls

MDAs must ensure that:

- each signatory is uniquely identifiable within the system used for signing;
- shared or generic signing accounts are not used;
- signatories maintain sole control over their credentials;
- authentication mechanisms are proportionate to transaction risk; and
- moderate and high-risk transactions use strong authentication measures.

11.2 Integrity and Tamper Evidence

MDAs must ensure that:

- electronically signed records are protected against unauthorised alteration or modification;
- any alteration or modification after signing is detectable; and
- signatures are invalidated where the integrity of the record cannot be assured.

11.3 Audit and Monitoring Controls

MDAs must ensure that:

- secure audit trails record the identity of the signatory, and the date and time of the signing action, together with relevant transaction details;
- audit logs are protected from unauthorised modification; and
- audit evidence supporting electronically signed records is retained in accordance with applicable records management and retention requirements.

11.4 Credential and Certificate Lifecycle Management

Where digital signatures or digital certificates are used, MDAs must ensure that:

- certificates are valid at the time of signing;
- revocation and suspension mechanisms are implemented;
- certificate expiry is monitored;
- renewal processes are documented;
- compromised credentials are promptly suspended or revoked; and
- affected transactions are reviewed where compromise is suspected.

Management of credential compromise must align with established ICT security and cybersecurity procedures.

12. Digital Certificates and Trust Framework

Where certificate-based digital signatures are used, MDAs must ensure that reliance on digital certificates is supported by applicable legislation, governance frameworks and validation mechanisms.

In particular, MDAs must ensure that:

- digital certificates are issued or recognised under an applicable certification framework consistent with the ETA ;
- mechanisms are in place to validate the status of digital certificates at the time of signing;
- revocation and suspension status can be verified;
- reliance on digital certificates is supported by documented trust policies; and
- verification of signatures can occur without exclusive dependence on proprietary software.

The detailed technical architecture and cryptographic standards applicable to digital certificates should be governed by technical standards issued by the ICT Authority or other competent authorities.

MDAs implementing certificate-based signatures should ensure alignment with guidance issued by the ICT Authority and with the applicable certification framework under the ETA.

13. Interoperability

Electronic signature solutions adopted by MDAs should support verification and reliance requirements across Government entities.

MDAs must ensure that electronically signed records can be independently verified from the originating system, especially for moderate and high-risk transactions.

Electronic signature implementations should comply with relevant GOJ ICT standards and digital governance frameworks issued by the ICT Authority.

Solutions should avoid relying solely on proprietary tools that hinder independent verification or validation across different entities.

14. Records Management and Long-Term Verifiability

Electronically signed records constitute official Government records and must be managed in accordance with applicable records management and archival requirements.

MDAs must ensure that electronically signed records are retained in a manner that preserves:

- the integrity of the record;
- the association between the signature and the record; and
- the supporting audit evidence required to demonstrate authenticity and reliability.

Where digital certificates are used for moderate or high-risk transactions, MDAs should ensure that mechanisms are in place to support long-term verification of the signature status, consistent with applicable retention periods.

Nothing in this Policy replaces or overrides existing records management laws, regulations, policies, procedures or retention schedules.

15. Acceptance of Electronic Signatures from External Parties

MDAs may accept electronic signatures from external parties where:

- the parties have agreed to transact electronically;
- the level of assurance is proportionate to the assessed risk of the transaction; and
- the authenticity and integrity of the electronically signed record can be reasonably validated.

Where electronic signatures are legally valid and meet the required assurance level, public entities should facilitate electronic submission processes in order to reduce unnecessary reliance on physical documentation.

In determining whether to accept an externally applied electronic signature, MDAs should consider:

- the nature and significance of the transaction;
- the identity assurance provided by the signature method; and

- any applicable procurement, contractual, or regulatory requirements.

Image-based signatures submitted by suppliers or other external parties may be accepted for low or moderate-risk transactions, provided that the identity of the signatory can be reasonably established and the authenticity and integrity of the record can be validated.

For high-risk transactions, MDAs should require digital signatures that provide assurance commensurate with the level of risk.

MDAs should avoid imposing vendor-specific requirements that unnecessarily restrict participation unless justified by the risk level and documented accordingly.

Acceptance of electronic signatures from external parties does not exempt MDAs from the duty to ensure transactions comply with relevant laws and governance standards.

16. Compliance and Review

MDAs are required to adopt electronic signature practices in accordance with this Policy. Non-compliance with this Policy may lead to administrative or governance repercussions under relevant public service, financial management, procurement, or ICT security frameworks.

Oversight of compliance should be part of each entity's existing internal control, audit, and governance mechanisms.

Repeated refusal to recognise valid electronic signatures, contrary to this Policy, may constitute a failure of internal control or administrative compliance.

This Policy will be reviewed tri-annually to incorporate legislative changes, technological advancements, and evolving governance needs.

End of Policy