Digital Signature Acceptance Policy

1.0 Purpose

As electronic communication and documentation become standard practice, digital signatures provide a mechanism for verifying the identity of a sender or signatory and ensuring message/document integrity. The purpose of this policy is to define when digital signatures are considered an acceptable and trusted substitute for traditional handwritten ("wet") signatures for internal organizational documents and correspondence, thereby reducing confusion and standardizing practice.

2.0 Scope

This policy applies to all employees, contractors, consultants, and other agents conducting business on behalf of the organization using organization-issued digital identities (key pairs). This policy specifically governs the use and acceptance of digital signatures on *intra-organizational* documents and correspondence (i.e., communications and documents shared solely within the organization). It does not cover electronic materials sent to or received from external parties unless explicitly stated otherwise in separate agreements or policies.

3.0 Policy Statements

3.1 Acceptance of Digital Signatures

* A digital signature applied using the organization's approved infrastructure and tools is considered an acceptable substitute for a wet signature on any intra-organizational document or correspondence, **except** for specific document types explicitly excluded by the organization.
* An official list of document types requiring traditional wet signatures (not covered by this policy) will be maintained by the designated financial or administrative authority (e.g., the Chief Financial Officer's office) and made available through designated internal resources (e.g., the organization's intranet).

3.2 Signature Validity

* Digital signatures must be associated with an individual user's identity. Digital signatures purporting to represent a role, position, or title (e.g., "Finance Department," "Project Manager") without being tied to a specific individual's key pair are not considered valid under this policy for authentication purposes.

3.3 Responsibilities

The effective use and acceptance of digital signatures rely on specific actions by both the signatory (signer) and the relying party (recipient).

*   **Signer Responsibilities:**
    *   Signers must obtain an official digital signing key pair issued through the organization's designated Identity Management group or process.
    *   This key pair must be generated and managed within the organization's approved Public Key Infrastructure (PKI), with the public key certified by the organization's designated Certificate Authority (CA).
    *   Signers must use only organization-approved software and tools for applying digital signatures.
    *   Signers have a critical responsibility to protect their private key from unauthorized access, loss, or disclosure. The private key must remain secret.
    *   If a signer suspects their private key has been compromised (e.g., stolen, lost, accessed by an unauthorized person), they must *immediately* report the compromise to the designated Identity Management group to initiate key revocation.
*   **Recipient Responsibilities:**
    *   Recipients must use organization-approved software and tools to view digitally signed documents or correspondence and verify the signatures.
    *   Recipients must verify the validity of a digital signature. This includes checking that the signature is cryptographically valid and that the signer's public key certificate was issued by the organization's designated CA and has not expired or been revoked. Verification is typically performed automatically by approved software, but recipients should understand how to check certificate details if needed.
    *   If a digital signature appears invalid, expired, revoked, or associated with an untrusted CA, the recipient must *not* trust the signature or the authenticity/integrity of the document based solely on that signature. Investigate further or request resubmission.
    *   If a recipient suspects misuse or forgery of a digital signature, they must report the concern to the designated Identity Management group or Information Security team.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team, Information Security, Internal Audit) will verify compliance with this policy through various methods, including audits of the PKI infrastructure, review of approved software lists, investigation of reported incidents, and user awareness checks.

4.2 Exceptions

Any exception to this policy (e.g., temporary use of alternative methods under specific circumstances) requires formal, documented justification and advance approval from the designated IT authority (e.g., Precision Computer team or Information Security).

4.3 Enforcement

Failure to comply with this policy, particularly regarding the protection of private keys or reporting compromises, may result in disciplinary action, up to and including termination of employment or contract. Misuse of digital signatures may lead to revocation of signing privileges and other sanctions.

5.0 Definitions

* **Digital Signature:** A cryptographic mechanism used to verify the authenticity (originator identity) and integrity (unaltered content) of electronic data.
* **Public Key Infrastructure (PKI):** A set of roles, policies, hardware, software, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
* **Certificate Authority (CA):** An entity trusted to issue, manage, and revoke digital certificates, which bind public keys to specific identities.
* **Key Pair:** In asymmetric cryptography, a pair of linked cryptographic keys: a public key (shared openly) and a private key (kept secret by the owner).
* **Private Key:** The secret component of a key pair used to create digital signatures and decrypt messages encrypted with the corresponding public key.
* **Public Key:** The publicly shared component of a key pair used to verify digital signatures created with the corresponding private key and encrypt messages for the private key holder.
* **Wet Signature:** A traditional, handwritten signature on a physical document.

Related Policies:

* Password Policy / Credential Management Policy
* Information Handling Policy
* Acceptable Use Policy
* (Potentially) Key Management Policy

Revision #2
Created 28 August 2024 16:50:39 by Daniel O
Updated 16 September 2025 22:10:08 by Travis Woolery