**Digital Signature Acceptance Policy**

# Overview

See Purpose.

# Purpose

The purpose of this policy is to provide guidance on when digital signatures are considered accepted means of validating the identity of a signer in ScaleArc electronic documents and correspondence, and thus a substitute for traditional “wet” signatures, within the organization. Because communication has become primarily electronic, the goal is to reduce confusion about when a digital signature is trusted.

# Scope

This policy applies to all ScalArc, Inc. (“ScaleArc” or the “Company”) employees and affiliates.

This policy applies to all ScaleArc employees, contractors, and other agents conducting ScaleArc business with a ScaleArc-provided digital key pair. This policy applies only to intra-organization digitally signed documents and correspondence and not to electronic materials sent to or received from non-ScaleArc affiliated persons or organizations.

# Policy

A digital signature is an acceptable substitute for a wet signature on any intra-organization document or correspondence, with the exception of those noted on the site of the Chief Financial Officer (CFO) on the organization’s intranet.

The CFO’s office will maintain an organization-wide list of the types of documents and correspondence that are not covered by this policy.

Digital signatures must apply to individuals only. Digital signatures for roles, positions, or titles (e.g. the CFO) are not considered valid.

## 4.1 Responsibilities

Digital signature acceptance requires specific action on both the part of the employee signing the document or correspondence (hereafter the *signer*), and the employee receiving/reading the document or correspondence (hereafter the *recipient*).

## 4.2 Signer Responsibilities

4.2.1 Signers must obtain a signing key pair from ScaleArc Operations Team. This key pair will be generated using ScaleArc’s Public Key Infrastructure (PKI) and the public key will be signed by the ScaleArc’s Certificate Authority (CA), scalearc.net.

* + 1. Signers must sign documents and correspondence using software approved by ScaleArc IT organization.
    2. Signers must protect their private key and keep it secret.
    3. If a signer believes that the signer’s private key was stolen or otherwise compromised, the signer must contact ScaleArc Identity Management Group immediately to have the signer’s digital key pair revoked.

## Recipient Responsibilities

* + 1. Recipients must read documents and correspondence using software approved by ScaleArc IT department.
    2. Recipients must verify that the signer’s public key was signed by the ScaleArc’s Certificate Authority (CA), <CA Name>, by viewing the details about the signed key using the software they are using to read the document or correspondence.
    3. If the signer’s digital signature does not appear valid, the recipient must not trust the source of the document or correspondence.
    4. If a recipient believes that a digital signature has been abused, the recipient must report the recipient’s concern to ScaleArc Identity Management Group.

# Policy Compliance

## 5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

# Related Standards, Policies and Processes

None.

# References

None.

# Definitions and Terms

None.

# Revision History

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| December 1, 2016 | Jacy York | Updated and converted to new format. |
|  |  |  |