NOVEMBER 2023

DIGITAL SIGNATURE POLICY

DRAFT VERSION 1.5

PRESENTED BY: ERIC SCHNELL, IT MANAGER

REVISED BY: ERIC SCHNELL
NIPISSING FIRST NATION

1. POLICY STATEMENT

Nipissing First Nation (NFN) will support all NFN staff with the option for digital signatures, whenever possible. Any section outlined within this document will not replace or override recommendations given by legal counsel. Any discrepancies found between this policy and legal council will be addressed in subsequent revisions of this policy.

2. PURPOSE OF THE POLICY

The purpose of this policy is to achieve the following statements:

- Increase productivity and efficiency
- Adopt environmentally friendly workflows
- Improve organization and member experience
- Ensure that electronic signatures are used in a way that establish necessary legal sufficiency

3. SCOPE

This policy applies to all NFN Staff and Chief & Council engaging in internal and external transactions involving signatures. It also applies to band members, members of the public, consultants, vendors, and other persons, when they engage in electronic transactions with NFN. This Policy applies only to transactions between NFN and the other person(s), each of which has agreed to conduct transactions by electronic means, as well as internal electronic processes, where the electronic signature is used.

4. DEFINITIONS

i. **"digital signature"** means a form of electronic signature that is fully or partially reinforced through cryptography to ensure the identity of the signer as well as the integrity and authenticity of a record.

ii. **"electronic signature"** means any electronic artefact that fulfils the function of a signature in the electronic medium. Electronic signatures may include, but are not limited to, digital signatures, name entries (online forms), email signature blocks or headers, click-through agreements, voice recordings, and combinations of a username and personal identification number (PIN).

iii. "**Identity Assurance"** determines the level of confidence required that the individual is who he or she claims to be.

iv. "**Credential Assurance"** determines the level of confidence required that an individual has maintained control over their credentials and that those credentials are not compromised.

v. **"Stakeholder"** any NFN decision maker who has a stake in the implementation of e-signatures within their department.

vi. **"Wet Signature"** means a signature made on a physical document using physical means.

5. USE OF ELECTRONIC SIGNATURES

5.1 To the fullest extent permitted by law, NFN accepts electronically signed documents as legally binding and having the same legal value as paper documents with handwritten signatures (wet signatures).

5.2 When there is no legal requirement that a document be signed, an electronic signature may be accepted instead of a digital signature.

5.3 This Policy does not limit NFN's right or option to conduct a transaction on paper or in a non-electronic form, nor affect the right or obligation to have documents provided or made available in paper format when required by statute or regulation.

5. INTERNAL DOCUMENTS AND TRANSACTIONS

Subject to the restrictions outlined in section "Documents Excluded", all internal documents of NFN, including but not limited to, official documents, requests, approvals, written communications, electronic submissions and transactions can be authorized or signed using electronic documents and signatures.

6. EXTERNAL DOCUMENTS AND TRANSACTIONS

All employees of NFN can accept the electronic submission of documents or transactions bearing an electronic signature if it is deemed to be in compliance with this policy.

7. EXCLUDED DOCUMENTS

The following documents shall not be signed in any circumstances using electronic signatures

a. Wills and codicils;
b. Power of Attorney;
c. Negotiable instruments (e.g. cheques, promissory notes, etc.);
d. Documents of title;
e. Affidavits;
f. Cash Distributions

8. CONSENT

8.1 No person shall be compelled or required to transact with the NFN using electronic signatures without their consent. If a handwritten signature (wet signature) is requested, NFN shall consent.

8.2 Consent does not have to be strictly expressed through an explicit communication. Rather, consent can also be inferred from a person's conduct if there are reasonable grounds to believe that the consent is genuine and is relevant to the information or document.

9. SOFTWARE USE

This Policy does not mandate any specific electronic signature software, so long as the application adopted meets the requirements outlined in this Policy. Any electronic signature software must undergo a review by the CEO, Director of Administration and the IT Manager before it can be adapted by NFN. The CEO will make final approval of any software before it can be adopted by NFN.

10. METHOD

10.1 The method of electronic signature used in a transaction will be determined based on:

- The reason or context of the signature;
- Risks or Assurance Level required by the particular type of transaction and the electronic record it is documented by.
- Legal Requirements
- Retention Requirements
- The ability of the method to validate the electronic signature through the retention period of the electronic record.

10.2 NFN shall not accept an electronic signing transaction if the method used by the other person does not meet the requirements outlined within this Policy.

11. DIGITAL SIGNATURE ASSURANCE AND METHOD SELECTION

To effectively manage risk, it's essential to determine the right type of signature for different scenarios. This decision is based on assurance levels, which indicate the degree of confidence needed in a digital signature's authenticity and integrity.

The assurance levels outlined here are inspired by guidelines from the Standard on Identity of Credential Assurance and the Government of Canada [1].

Assurance Levels:

- **Level 1: Basic Assurance**
    - Confidence Needed: Minimal.
    - Risk: Minimal to no harm if compromised.
    - Suitable Method: **Basic Electronic Signature.** For instance, a user clicks a checkbox to agree or approve. Think of simple online form submissions without major legal consequences.
- **Level 2: Moderate Assurance**
    - Confidence Needed: Some.
    - Risk: Minimal to moderate harm if compromised.
    - Suitable Method: **Electronic Signature with Authentication.** Used for most internal processes, such as Microsoft authenticated forms, approvals, or automated workflows.

- **Level 3: High Assurance**
    - Confidence Needed: High.
    - Risk: Moderate to serious harm if compromised.
    - Suitable Method: **Digital Signature via Established Platforms** like DocuSign or Adobe Sign. Ideal for external transactions where parties can't use standard credentials, like contracts with vendors or agreements with members.
- **Level 4: Very High Assurance**
    - Confidence Needed: Very high.
    - Risk: Serious to catastrophic harm if compromised.
    - Suitable Method: **Wet Signatures or Advanced Digital Methods** as indicated by law or as listed in the "Excluded Documents" section. Used for critical documents or those mandated by law.

For detailed definitions and technical background on these levels, refer to Appendix A.

When selecting a digital signature solution or auditing existing ones, use the above guidelines to ensure that the software meets the required assurance level.

Approved this 19th day of December, 2023.

APPENDIX A: EXAMPLES OF HARM

Category of Harm	Level 1	Level 2	Level 3	Level 4
Inconvenience, distress, loss of standing or reputation	An inconvenience, distress or damage to the standing or reputation of any party Alternatives are available with little or no delay and no additional costs or degradation of service quality Minor embarrassment	A **serious short-term or a limited long-term** inconvenience, distress or damage to the standing or reputation of any party Alternatives are readily available Loss of reputation or standing between the principals Loss of trust or confidence between principals	A **serious long-term** inconvenience, distress or damage to the standing or reputation of any party Alternatives are not readily available Loss of reputation or standing beyond the principals (including third parties) Loss of trust or confidence beyond the principals (including third parties)	A **severe and permanent** inconvenience, distress or damage to the standing or reputation of any party Alternatives are not available Wide-scale permanent loss of reputation or standing Wide-scale permanent loss of trust or confidence
Financial loss (Note: The severity of the loss depends on the impact of the loss on the affected party)	A financial loss No financial loss	A **minor** financial loss to any party Financial loss that has no impact or only an insignificant material impact on the financial standing of an individual or organization A budgetary impact that may require reallocation of funds but no additional financing	A **major** financial loss to any party Loss of a financial amount that has a significant material impact on the financial standing of an individual or organization. A budgetary impact that may require re-allocation of funds and additional financing.	An **extreme** financial loss to any party Loss of a financial amount that severely jeopardizes the financial standing of an individual or organization Financial restructuring may be required.

Harm to program, department, asset or public interest	An adverse effect on the program, department, asset or public interest No noticeable reduction in effectiveness of a primary function of an organization No compromise to a critical asset No loss of public confidence	A **limited adverse effect** on the program, department, asset or public interest it can perform its primary function but with reduced effectiveness No compromise mise to a critical asset Temporary loss of public confidence	A **serious adverse effect** on the program, department, asset or public interest it can perform its primary function with significantly reduced effectiveness Compromise to a critical asset Long-term loss of public confidence	A **catastrophic adverse effect** on the program, department, asset or public interest it is unable to perform its primary function Major damage to or potential loss of a critical asset Permanent loss of public confidence
Unauthorized release of sensitive band information	A loss of confidentiality No increase in public scrutiny or media attention	A **limited adverse effect** on band operations due to a loss of confidentiality resulting from the release of sensitive band information to unauthorized parties Loss of public confidence Increase of public scrutiny or media attention Diminished program integrity	A **serious adverse effect** on band operations due to a loss of confidentiality resulting from the release of sensitive band information to unauthorized parties Increased oversight (e.g., increased audits, more stringent approval processes) Temporary revocation of departmental authorities Compromise to critical asset	A **catastrophic effect** on organizational band operations due to a loss of confidentiality resulting from the release of sensitive band information to unauthorized parties Loss of continuity of critical band services Major damage to or potential loss of a critical asset Irreversible damage to public trust

Civil or criminal violations	(Any compromise involving a legal violation is assessed at a minimum of Level 2)	A **violation** that may have **minor consequences** False claims or wrongful actions having minor financial or legal implications and which pertain to the individual only The violation does not ordinarily require disciplinary, investigative or enforcement action The violation may result in a summary offence	A **violation** that may have **serious consequences** False claims or wrongful actions significant financial or legal implications and which may also pertain to third parties (e.g., trustees acting on behalf of the individual) Violation could require disciplinary, investigative or enforcement action. The violation may result in an indictable offence	A **violation** that may have **exceptionally grave consequences** False claims or inaccurate representations in relation to services or transactions where the safety and well-being of the individual or other affected parties may be jeopardized The violation requires disciplinary, investigative or enforcement action. The violation may result in an indictable offence of a serious nature
Assurance Level Requirement	Minimum Level 1 Required if any of the above applies	Minimum Level 2 Required if any of the above applies	Minimum Level 3 Required if any of the above applies	Minimum Level 4 Required if any of the above applies

12.REFERENCES

[1] "Guidline on Defining Authentication Requirements," Government of Canada, 30 November 2012. [Online]. Available: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26262&section=html. [Accessed 23 July 2021].