Subject to significant changes

SPECIAL CONDITIONS OF USE FOR PRODUCTS OFFERED BY SOLUTIONS NOTARIUS - CERTIFIO® (hereinafter referred to as the "Special Conditions")

Between **SOLUTIONS NOTARIUS INC.**, a Portage Cybertech company, having its head office at 465 McGill Street, Suite 300, Montreal, Quebec, Canada H2Y 2H1 ("**Notarius**") and you (hereinafter referred to as "**you**," "**Purchaser**," "**Holder**," "**Organization**," "**Entity**," or "**Recognized Professional Association**," as the case may be) (individually referred to as a "**Party**" and jointly referred to as the "**Parties**").

Since 1998, the Notarius Certification Authority (CA), based on a Public Key Infrastructure (PKI), has been recognized and trusted by various government agencies. In 2007, Notarius became the first Certification Authority in North America to be certified to ISO 27001 (information security management). A pioneer in digital trust, Notarius is an active member of the Digital Identification and Authentication Council of Canada (DIAC), the Federation of Digital Trusted Third Parties (FDTT) and the PDF Association. Notarius is the only Canadian company to issue trusted Digital Signatures certificates recognized by Adobe (Adobe Approved Trust List - AATL) and Microsoft (Microsoft Trusted Root Certificate Program).

As a certificate and repository services provider ("C/RSP"), Notarius has long been dedicated to offering Digital Signature solutions (digital signature certificates on .epf or cryptographic token) to ensure the long-term reliability of documents.
Keeping at the forefront of technology and attentive to stakeholders' needs and given the evolving technology – specifically the ever-more important place of Cloud computing and mobile technology – Notarius felt an obligation to improve its Product offering. As such, Notarius's new Digital Signature Cloud Solution, "*CertifiO Cloud*," allows Holders to digitally sign documents without needing to first install elements of the signing certificate (for example, the private key) locally on their workstations.
Notarius also offers its clients a solution for securing documents by barcode, the visible digital seal (VDS), "*CertifiO Code,*" which includes electronically signed key data to detect any alteration and to confirm the issuer's authenticity and legitimacy.

Notarius grants you, in return for the payment of the required sums, a non-exclusive licence, which is not transferable and not assignable to a third party in whole or in part, to use CertifiO according to the terms and conditions described below.

By subscribing to and using CertifiO, you consent and accept these Special Conditions.

1. GENERAL CONDITIONS

THESE SPECIAL CONDITIONS SUPPLEMENT THE **GENERAL TERMS OF USE** AND TOGETHER THEY GOVERN YOUR USE OF CERTIFIO. THE GENERAL TERMS OF USE SHALL BE DEEMED TO FORM AN INTEGRAL PART HEREOF.

1.1. Products from the CertifiO product suite allow Holders to digitally sign their documents. All CertifiO products include the necessary licenses and signing certificates to sign your electronic documents to preserve the origin, integrity, and authenticity of the signed document.

1.2. Products from the CertifiO product suite allow you to obtain and use a Digital Signature certificate following an identity verification or entity verification, and certification of your professional status or employment relationship, when applicable.

1.3. Documents signed with a Product from the CertifiO product suite allow you to certify a signer's identity as well as their professional status or affiliation to an Organization.

1.4. To be authorized to subscribe to Products in the CertifiO product suite, your employer must first have opened a corporate account with Notarius. In addition, only an email address containing a combination of your first and/or last name and linked to this employer should be used when you are subscribed to the Product.

2. DEFINITIONS

Terms not defined in these Special Conditions have the meanings ascribed to them in the General Terms of Use or in Notarius's Certificate Policies or Certification Practices Statements.

2.1. "**AATL or *Adobe Approved Trust List***": As defined by Adobe, a program (referring to a list of authorized service providers) that allows millions of people around the world to digitally sign documents using the most trusted digital identities. Certificate authorities (CAs) and Trusted Third Parties on the AATL list issue digital certificates allowing for certified timestamps and the affixing of signatures linked to trusted digital identities in compliance with the highest legal and regulatory requirements worldwide. AATL is an Adobe feature offered for some, but not all, Notarius digital signatures resulting in the default recognition of Notarius signatures in all Adobe software.

2.2. **"Certificate and Repository Services Provider (C/RSP)":** Entity responsible for administering certificate and repository services associated with certificate issuance and management.

2.3. **"Certificate Authority (CA)":** Entity responsible for certificates signed in its name as well as the PKI.

2.4. **"Certificate Policy (CP)":** A set of rules, identified by an object identifier (OID), setting out the requirements that bind the CA in the implementation and delivery of its services. These official documents are available on the Notarius website here: https://www.notarius.com/en/certification-policies-and-practice-statements.

2.5. "**CertifiO Code":** A digital signature certificate signing the VDS to ensure its integrity and authenticity. Issued for one or more specific use cases as authorized by AIGCEV. Issued to organizations generally responsible for issuing documents to which the VDS will be affixed. Used in conjunction with

ConsignO® Server and VerifiO® solutions, you can create, affix, and validate a VDS on a printed document to ensure its integrity and authenticity.

2.6. **"CertifiO for Departments":** Digital signature certificate certifying the name of the department of an Organization and associating the document signed with the certificate to that department. An employee signs on behalf of the Organization, for a maximum of 2,000 signatures annually. Information about the signer's identity is not included in this certificate.

2.7. **"CertifiO for Employees**": Digital signature certificate for employees certifying the Holder's identity and employment relationship with a Notarius client Organization. This digital signature certificate is for the exclusive use of the Holder identified in the certificate.

2.8. **"CertifiO for Evaluation"**: Digital signature certificate for testing purposes only; may not be used in a different context. Does not certify the signer's identity, professional status, or relation to the employer. The certificate includes metadata which indicates to Adobe Acrobat and ConsignO that the signer's identity has not been verified and is therefore not reliable.

2.9. **"CertifiO for Organizations":** Certifies the organization from which the document originated. This type of digital signature certificate is typically integrated into an automated process on a server for large volumes of documents signed annually. This subscription is based on the annual volume of signed documents and requires a corresponding lot of licenses. Digital signature certificates for Organizations are always AATL.

2.10. **"CertifiO for Professionals**": Digital signature certificate certifying the signer's identity and professional status. This digital signature certificate is for the exclusive use of the individual named in the certificate. The membership number and legal name of the Recognized Professional Association is indicated in the Certificate. This type of Product requires the signing of a formal agreement between Notarius and the Recognized Professional Association.

2.11. **"Client application**": An application or software program installed on the Holder's workstation or accessed online through which the Holder can activate or recover certificates, change their password, perform configuration tasks, and make transactions using their certificates.

2.12. "**Digital Signature Software**": Software used to cryptographically bind a digital signature certificate to a document. Users are free to use any standards-compliant digital signature software that can access and use digital signature certificates.

2.12.1. Notarius provides **Digital Signature Desktop Solution** Holders with digital signature software, marketed as *ConsignO Desktop*, allowing you to perform the following advanced operations:

a) Create and save Digital Signature zone templates;
b) Digitally sign documents, including the batch signing; and
c) Convert and verify compliance with the PDF/A standard.

2.12.2. Notarius provides **Digital Signature Cloud Solution** Holders with a Web Application, marketed as *ConsignO Cloud Solo*, which allows you to digitally sign using your individual CertifiO Cloud digital signature to produce a highly compliant document. You are granted access to this application by way of authentication of your Notarius account ("My Account") following subscription to the CertifiO Cloud product.

2.13. "**Escrow Agreement**": For a supplier of a product or service, it consists in entrusting to a third-party escrow essential elements (software, databases, documents, etc.) for the use of this product or the realization of this service. The objective is to ensure that a third party (customer, partner, etc.) has access to them, according to the provisions agreed between the parties, and in particular in the event of the supplier's failure.

2.14. **"Hosted HSM"**: The digital signature certificate, part of the CertifiO for Organizations (AATL) solution, is hosted on an HSM certified by Notarius that can be remotely queried to sign data using the Entity's certificate (i.e. organization). This type of subscription is based on the annual volume of documents signed and requires a corresponding Lot of signatures.

2.15. **"Identity Verification Agent (IVA)**": C/RSP employee authorized to carry out identity verifications (IV) of natural persons who are Purchasers of certificates according to the specifications detailed in the Notarius Certificate Policy (specifically, the completion of a web form specific to the Product purchased and the scheduling of an appointment for the purpose of presenting the required proof of identity). In some cases and under certain conditions, organizations may benefit from a special authorization to carry out identity checks themselves. In this case, an Identity Verification Agent (IVA) and an Affiliate Verification Agent (AVA) must be expressly appointed. For example, for notaries, the IV must be completed by a notary in accordance with Section 3 of the *Regulation respecting the digital official signature of a notary*, CQLR c N-3, r.13.1. 13.1.

2.16. **"Key compromission":** A private key is compromised when its value has been disclosed to an unauthorized person, if an unauthorized person has had access to it, or if there is a method by which an unauthorized person can discover its value.

2.17. **"Key pair"**: A key pair is a combination of a private key (to be kept secret) and a public key, both of which are required to execute cryptographic functions based on asymmetric algorithms.

2.18. **"My Account"**: The Notarius account is a secure online account (username/password) allowing the Holder secure access to the different Products offered by Notarius (for example, the My Account administrative portal and the CertifiO Cloud Signature). Furthermore, My Account includes features to manage the life cycle of the Client's Digital Signature**.**

2.19. "**PDF/A**": The ISO 19005 standard ensures that electronic documents can be opened and read over long periods of time.

2.20. **"Private key":** The key in a key pair that is kept secret by the key pair holder and is used to create digital signatures or to decrypt documents that have been encrypted with the corresponding public key.

2.21. **"Public key":** The key in a key pair that may be publicly disclosed by the holder with a corresponding private key and that is used by a user party to verify digital signatures created with the holder's corresponding private key or to encrypt a document, for example, so that it can be decrypted only with the holder's corresponding private key.

2.22. **"Public Key Infrastructure (PKI)":** Set of physical components, functions, and procedures performed by software and human resources to manage keys and certificates issued by the CA.

2.23. **"Revocation":** The withdrawal of a Holder's certificate performed at the discretion of the C/RSP or at the request of an authorized individual.

2.24. **"Visible Digital Seal (VDS)"**: A data structure that guarantees the origin and integrity of a document's key data by encapsulating the data with its organizational (or departmental) digital signature in a two (2) dimensional code. The VDS to which the Notarius CP refers is the Otentik VDS, whose governance is dictated by AIGCEV.

3. RESPONSIBILITIES AND OBLIGATIONS OF THE END USER, HOLDER, PURCHASER, ENTITY, ORGANIZATION, RECOGNIZED PROFESSIONAL ASSOCIATION, OR ITS AUTHORIZED AVAS

Products in the CertifiO product suite allow you to affix a digital signature certifying your identity or that of the signing department or organization, as well as your professional status or employment relationship when applicable.

As such, you consent, accept, acknowledge, and agree to:

3.1. Use Notarius Products in accordance with the obligations herein including the General Terms of Use and those described in the Certificate Policies and Certification Practices Statements adopted by Notarius.

3.2. Provide to Notarius true, accurate, current, and complete information and/or Personal Information. promptly update your Information and/or Personal Information (such as your email address or telephone number) when required.

3.3. Provide an email address containing a combination of your first and/or last name and linked to your employer when you subscribe to the CertifiO for Employees Product (both Cloud and Desktop).

3.4. Provide, for all requests to subscribe to CertifiO Products including for Organizations, Departments, VDS, or to open a company account, the official and active legal name of your Organization as registered with the competent authorities (for example, a business registry). If your organization is registered in a province where access to the registry is paid or abroad, you agree to attach to your application a recent official copy of the register proving its legal existence in one of Canada's two (2) official languages (English or French).

3.5. Book your identity verification with an authorized IVA, which will perform the necessary verifications and collect some of your personal information. This information will be processed in accordance with the Notarius Privacy Policy and Certification Policy.

3.6. Present original, valid proofs of identity issued by a recognized government authority during your identity verification with the authorized IVA.

3.7. Authorize Notarius to use your Personal Information for identification purposes in connection with the provision of the Products. For details regarding the Identity Verification, see the Notarius Certification Practices Statements for the Product purchased.

3.8. You are solely responsible for protecting the confidentiality of your password, identification codes, security questions, and answers needed to identify you and giving you access to the My Account section. You may lose access to the Products in the event that you lose your password.

3.9. The use of your Digital Signature is a PERSONAL RIGHT, and it is STRICTLY FORBIDDEN to entrust or disclose to anyone else the information that enables its use. A breach of this obligation may not only result in the revocation of your Digital Signature Certificate without further notice or delay but may also be reported immediately and without further notice to your Order or Professional Association for Digital Signature Holders for Professionals.

3.10. You acknowledge that your Personal Information (including contact information) may be used by third parties who wish to provide Notarius with proof that your private key has been compromised (e.g., by signing a certificate revocation request using that private key) so that your corresponding Digital Signature certificate can be revoked.

3.11. Validate that the signature appearance applied to your document complies with the requirements of your Recognized Professional Association. You also agree to sign with the signature appearance associated with the selected digital signature in cases, for example, where you hold multiple digital signatures (both Desktop and Cloud).

3.12. If you have purchased an annual certificate for a hosted HSM, you agree to ensure that your Client:

3.12.1. Agrees to comply with the Products' Terms of Use and Notarius's dedicated Certificate Policy.
3.12.2. Attaches a recent, up-to-date, and valid copy from the appropriate business registry to prove its legal existence.
3.12.3. Provides truthful, accurate, and complete information and/or Personal Information, and notifies you of any changes to the information contained in the certificate.
3.12.4. Is responsible for the inappropriate use of its keys by its employees, administrators, or others.
3.12.5. Acknowledges and agrees that (i) you are solely responsible for protecting the Organization's login information, including but not limited to its username/password or API signing key/secret, as applicable; (ii) if applicable, acknowledges and agrees that it is possible for you to delete Signature Projects from its account or to transmit or send Signature Projects to an incorrect recipient; (iii) if applicable, acknowledges and agrees that you may have access to the signing certificate and key and, in that respect, that you alone are responsible for the improper use of such keys; (iv) releases Notarius of any liability for the incorrect use of its Certificate by you.

3.13. Comply with, and have End Users comply with, the licences of Notarius's licensors contained in the CertifiO suite.

3.14. Be responsible for establishing the necessary configuration, including obtaining and paying for the equipment and third-party services required for your access and use of the Services, including but not limited to Internet access.

3.15. Be fully responsible for implementing internal administrative policies and practices to prevent unauthorized access, use, modification, or disclosure of the Products by unauthorized Parties using equipment under your control.

3.16. Notify Notarius immediately if there is any suspicion of a Key Compromission or loss of your Digital Signature certificate.

3.17. Train your End Users, when applicable, and ensure that they use the Products in accordance with the directives issued by Notarius from time to time.

3.18. Provide accurate, exact, and complete information and inform Notarius of any change as soon as possible, including any change within your organization or the temporary or permanent revocation of a Holder or an End User authorized to act in your name and use the Products.

3.19. Verify the validity or revocation of your Digital Signature using the current certificate revocation status or subscription status information identified in "My Account". Furthermore, DO NOT USE the medium that contained the revoked Digital Signature certificate.

3.20. Approve or reject subscription requests when required. Approval includes confirmation of the employment relationship when applicable.

3.21. Revoke certificates when the employment relationship ceases to exist, or the Holder is no longer an active member of the Recognized Professional Association.

4. NOTARIUS'S RESPONSIBILITIES AND OBLIGATIONS

4.1. Supply of the Products. Subject to payment of all applicable fees and compliance with all Terms and Conditions, including the Special Conditions, Notarius undertakes to supply the Products to the Purchaser and such Products shall be fully provided in accordance with their Product Specifications. The Purchaser also accepts that the Products may be supplied, in whole or in part, by a third party.

4.2. Certificate Authority. Notarius acts as Certificate Authority or Service Provider. As such, Notarius is responsible for issuing Digital Signatures and conducting the necessary verifications before issuing them.

4.3. Identity Verification. To issue a Digital Signature, Notarius must verify (except for the exception mentioned in section 2.2) the identity of the Holder and/or End User, as the case may be. Therefore, some Personal Information must be disclosed to Notarius, as specified in the directions given to the Holder and/or End User to this effect. You authorize Notarius to use this Personal Information to provide the Products. You also authorize Notarius to keep evidence of your identity verification for a minimum of 10 years from the anniversary date of the cancellation of your subscription.

4.4. Digital Signature Event Logs. Event logs related to your Digital Signature are retained for a minimum of 10 years from the anniversary of the expiration or revocation of your Certificate.

4.5. If key pairs are generated by Notarius on behalf of the Purchaser and offered in PKCS#12 format, Notarius will endeavour to use trusted systems to generate the key pairs including a platform recognized as suitable for this purpose, ensure that private keys are encrypted if sent to a Holder, use a key length and algorithm that are recognized as suitable for the purpose of the digital signature, and will not sign key pairs less than 2048 bits for VDSs.

4.6. Escalation of Security Breaches to your Professional Association. In accordance with 3.9, Notarius may be required to notify the Holder's Professional Association in the event of a suspected or proven compromise of the Holder's Digital Signature Certificate.

5. SPECIFIC PROVISIONS FOR CERTIFIO FOR PROFESSIONALS

5.1. Price Modifications by a Recognized Professional Association: Recognized Professional Associations that bill their respective members for services related to the CertifiO for Professionals Product reserve the right to modify their own prices at any time. Such price modifications will apply immediately and must be communicated by the Recognized Professional Association to their members through a written notice to this effect. If the Client refuses this increase, it may revoke its CertifiO for Professionals Digital Signature through "My Account."

6. END OF AC LIFE AND ESCROW

6.1. If CRLs are provided and Notarius removes revoked certificates from the CRL after they have expired, the CRL will not include the X.509 extension "ExpiredCertsOnCRL" as defined in ISO/IEC 9594-8/Recommendation ITU T X.509.

6.2. If CRLs are provided and Notarius decides or is required to terminate a CRL, it shall issue and publish at the corresponding CRL distribution point a final CRL with a nextUpdate field value as defined in ETSI EN 319 411-1 [2], clause 6.3.9. Requirement CSS-6.3.9-06.

6.2.1. CRL termination may occur when there are no more valid certificates in the CRL scope, such as when the CRL Signing Entity certificate expires or when the CRL Signing Entity private key is downgraded.

6.3. The OCSP responder uses the ArchiveCutOff extension as specified in IETF RFC 6960, with the archiveCutOff date set to the notBefore date and time value of the CA certificate.

6.4. In the event of CA compromise, Notarius shall broadcast a CA revocation status CRL with the updated revocation status on the distribution points already defined.

6.5. In case of CA end of life, the CRL issued by Notarius will be issued with a NextUpdate field value of 99991231235959Z.

6.6. Notarius will not issue a final CRL until all certificates covered by this CRL have expired or been revoked.

Last updated: September-22-2023