

SIGNATURE ÉLECTRONIQUE DES DOCUMENTS

Recommandations aux unités

Mise à jour : Juin 2022

Le secrétariat général souhaite formuler des recommandations générales concernant la signature électronique.

Définitions

La principale fonction d'une signature est de prouver l'identité du signataire, son intention de signer, et son intention d'être lié juridiquement par le contenu du document¹.

Les formes de signature électronique sont multiples : image de signature manuscrite, signature via une plateforme web, signature via un certificat numérique, etc. Une signature électronique sécurisée permet de garantir à un document numérique son origine, son intégrité et son authenticité². Une signature sécurisée est requise lorsqu'on signe des documents constitutifs de droits et/ou obligations pour l'Université, car ce type de signature :

- permet d'attester l'identité de l'émetteur du document;
- assure l'authenticité des signatures en prouvant que c'est la personne visée qui a signé le document;
- permet de garantir l'intégrité du document, en attestant qu'il n'a pas été modifié depuis la signature;
- en préserve la pérennité en veillant à ce qu'il demeure valide dans le temps.

Chaque type de signature électronique revêt un caractère de fiabilité juridique différent; par exemple, une image d'une signature manuscrite ne permet pas de prouver l'identité du signataire et n'est pas opposable en cour de justice. Avant de signer un document, il est donc important de prendre en compte le contexte et les besoins en termes de fiabilité juridique, afin de choisir le type de signature électronique adéquat.

Voici quelques exemples de signature électronique :

TYPE DE SIGNATURE	EXEMPLES	NIVEAU DE SÉCURITÉ
Signature électronique simple	Image de signature manuscrite, case à cocher, etc.	Faible

¹ Orientation du gouvernement du Canada sur l'utilisation des signatures électroniques, Secrétariat du Conseil du Trésor du Canada, publication initiale 15 juillet 2019 : <https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/securite-confidentialite-ligne/orientation-gouvernement-canada-utilisation-signatures-electroniques.html>

² Pour plus d'information : <https://www.notarius.com/fr/bibliotheque/comment-les-signatures-electroniques-se-differencient>

TYPE DE SIGNATURE	EXEMPLES	NIVEAU DE SÉCURITÉ
Signature électronique avancée	<p><u>Signature via le login UdeM</u> Exemples : signature via les modules Synchro; signature par autorisation écrite en utilisant le courriel institutionnel</p> <p><u>Déclaration solennelle</u> Exemple : courriel comportant la mention suivante : « <i>Je déclare solennellement que les renseignements fournis dans le présent document sont véridiques, exacts et complets. Je reconnais que cette déclaration a la même force et le même effet qu'une déclaration faite sous serment en conformité avec les lois applicables.</i> » Ce type de signature peut accompagner des documents dans le cadre de processus internes (par ex. : transactions, budgets, listes, procès-verbaux, etc.).</p>	Modéré
Signature électronique qualifiée	<p>Signature électronique via les produits des entreprises de signature électronique sur le marché : signature via une plateforme web, signature via un certificat numérique (clés de signature) Exemples : Notarius, Adobe, DocuSign, eZsign, etc.</p>	Élevé

Plateforme de signature ConsignO Cloud

L'Université utilise la plateforme ConsignO Cloud de l'entreprise Notarius, fondée par la Chambre des Notaires du Québec. La plateforme doit être utilisée uniquement pour la signature électronique de **contrats, ententes ou conventions comportant un engagement légal avec des parties externes**.

Tableau-synthèse

À titre indicatif, ce tableau présente les principales catégories de documents signés à l'Université, avec des recommandations du type de signature et d'outil à utiliser.

TYPES DE DOCUMENT	TYPES DE SIGNATURE	COMMENTAIRES
<p>Documents relatifs aux transactions diverses dans les modules Synchro-Finances, RH, Académique, Recherche (bourses et prix, comptes de dépenses, paiements aux fournisseurs externes et sur fonds de recherche, contrats d'engagements, relevés de notes, attestations d'inscriptions et d'études, etc.)</p>	Signature électronique avancée (via Synchro)	Le login de l'utilisateur UdeM dans Synchro authentifie l'auteur et permet de certifier la signature dans le système.

TYPES DE DOCUMENT	TYPES DE SIGNATURE	COMMENTAIRES
Contrats, ententes et/ou conventions avec des parties externes (documents externes comportant un engagement légal)	Signature électronique qualifiée : ConsignO Cloud	Ces documents sont créateurs de droits et/ou obligations pour l'Université avec des parties externes. Ils doivent être signés au moyen de ConsignO Cloud, la solution technologique retenue par l'Université, puis transférés à la DGDA.
Documents/formulaires non contractuels destinés à l'externe (lettres d'intention, de recommandation, lettres d'appui financier, applications pour un programme/bourses, etc.)	Dépend du type de document. Tout type de signature électronique peut être accepté. Parfois, le destinataire peut exiger un type de signature spécifique (ex. : signature par un certificat numérique)	L'appréciation est à la discrétion du signataire.
Documents issus des instances universitaires (procès-verbaux et extraits)	ConsignO Cloud ou autres outils technologiques avec signature sécurisée Déclaration solennelle	Documents signés en format PDF/A à transmettre à la DGDA
Documents/formulaires non contractuels destinés à l'interne (correspondance courante, formulaires divers)	Dépend du type de document. Tout type de signature électronique peut être accepté.	L'appréciation est à la discrétion du signataire.

Principes directeurs et bonnes pratiques

Principes directeurs

- Comme mentionné précédemment, l'usage des différentes signatures électroniques varie en fonction du type de document à signer. Ainsi, les membres du personnel ont la responsabilité d'analyser leurs besoins en termes de fiabilité et d'authenticité du document afin de choisir le type de signature électronique adéquat.
- Les documents de nature contractuelle doivent être signés via la plateforme ConsignO Cloud.
- Les documents constitutifs de droits et/ou obligations pour l'Université devraient être signés au moyen d'outils technologiques reconnus (tels que ConsignO Cloud), dans la mesure du possible. Diverses solutions technologiques utilisant des certificats de signature numérique qualifiée existent sur le marché (par ex. Adobe, DocuSign, eZsign, etc.) et sont conformes du point de vue sécurité de la signature.
- Certains documents doivent être convertis au format PDF/A avant d'apposer une signature, afin de garantir leur intégrité, authenticité et favoriser leur préservation. La procédure à suivre est disponible sur le site web de Division de la gestion de documents et des archives (DGDA) à l'adresse suivante : https://archives.umontreal.ca/fileadmin/archives/doc/gd/Procedure_conversion_PDF-A.pdf

- Les autres documents, notamment ceux qui ne lient pas légalement l'Université et les membres de son personnel, peuvent être signés de manière non sécurisée.

Bonnes pratiques

- Les meilleures pratiques en matière de signature électronique proscrivent la délégation de la signature personnelle à des tiers, puisque l'objectif d'une signature électronique sécurisée est de garantir l'identité de l'émetteur du document et l'authenticité de ce dernier.
- Les membres du personnel devraient appliquer des mesures de contrôle visant à garantir la sécurité de leur signature électronique (par exemple : ne pas communiquer leur clé de signature personnelle à des tiers, la conserver dans un endroit sécurisé en tout temps, utiliser un mot de passe complexe, etc.).
- Il existe des délégations de pouvoir et de signature dans le cadre de certains processus administratifs à l'Université³. Les personnes déléguant leur signature devraient alors s'assurer, d'une part, que la signature est apposée par la personne délégataire autorisée et, d'autre part, que cette personne respecte les principes directeurs susmentionnés.

Conservation des documents numériques

Conformément à la *Politique sur la gestion de documents et des archives* (10.49), chaque unité de l'Université a la responsabilité d'appliquer le [Programme de gestion intégrée de documents](#) élaboré par la Division de la gestion de documents et des archives. L'une de ces responsabilités est notamment de procéder au transfert, au versement ou à l'élimination des documents, y compris les documents numériques, en respectant les règles de gestion des documents. La DGDA met à la disposition des unités une voûte documentaire institutionnelle dans laquelle les documents numériques à valeur patrimoniale doivent être déposés : le logiciel **SyGED**. Les documents contractuels ainsi que les procès-verbaux des organismes de l'Université doivent quant à eux être transférés à la DGDA dès leur signature conformément à la *Directive concernant l'archivage des contrats* (10.6.1) et à la *Directive relative à la création et à la conservation des procès-verbaux et des dossiers-séances des organismes de l'Université* (40.26). Tel que mentionné, il est important de convertir ces documents en format PDF/A avant signature en vue de leur transfert à la DGDA.

Ressources complémentaires

Politiques et directives de l'Université

- [Politique de gestion de l'information](#) (10.47);
- [Politique sur la gestion de documents et des archives](#) (10.49);
- [Règlement sur les autorisations de conclure et de signer des contrats au nom de l'Université de Montréal](#) (10.6);
- [Directive concernant le stockage de l'information institutionnelle en infonuagique](#) (10.54)
- [Directive concernant l'archivage de contrats](#) (10.6.1)
- [Directive relative à la création et à la conservation des procès-verbaux et des dossiers-séances des organismes de l'Université](#) (40.26)

³ Par ex. les formulaires Synchro de demandes d'accès de délégués; certains formulaires de la Direction des finances (DF) – signataires autorisés pour les fonds de fonctionnement sans restriction, demandes de dérogation aux directives de la DF pour des délégations de signature, etc.

Ressources de la Division de la gestion de documents et des archives

- Site web de la DGDA : <https://archives.umontreal.ca/accueil/>
- [Programme de gestion intégrée de documents](#)
- [Règles de gestion des documents](#)
- [Procédure de transfert de procès-verbaux](#)

Ressources concernant ConsignO Cloud

Comment se procurer ConsignO Cloud?

Il n'est pas nécessaire de posséder un compte utilisateur pour être en mesure de signer les documents; seules les personnes devant préparer et envoyer des documents à signer sont invitées à se procurer ConsignO Cloud. Pour accéder à la plateforme, les membres du personnel doivent en faire la demande auprès du responsable informatique de leur unité. Plus d'informations sont disponibles sur la [page Wiki des TI](#). À noter que la plateforme est compatible avec tous les systèmes informatiques (PC, Mac, Android, iPhone, etc.).

Ressources complémentaires de Notarius :

- [Vidéo de présentation de ConsignO Cloud](#)
- [Guide d'utilisation en ligne](#)
- [Formation en ligne gratuite dispensée par Notarius](#)

Service de soutien à la clientèle :

- Centre d'aide Notarius <https://support.notarius.com/>
- Assistance technique par courriel: support@notarius.com
- Clavardage disponible sur <https://www.notarius.com/fr/>
- Service à la clientèle disponible par téléphone du lundi au vendredi de 8h30 à 19h00 au +1 855-505-7272

Pour plus d'information

Veillez communiquer avec la [Division conformité et gestion des risques](#) pour du soutien additionnel concernant la conformité et les outils de signature électronique.