Université Concordia University

RECORDS MANAGEMENT
AND ARCHIVES

Electronic Signature Framework

Prepared by

Marie-Pierre Aubé, University Archivist

September 2021

CONCORDIA

E-Signature Framework

Table of Contents

1. Purpose

This Framework outlines the process for using electronic signatures at the University for all employees. It indicates the cases and documents in which the electronic signature can be used.

This Framework operates within the scope of the *Policy on Contract Review, Signing and Required Approvals* (BD-1), *Policy on Information Security* (VPS-33) and *Policy on Records Management and Archives* (SG-10).

Objectives:

- To define electronic signature.
- To establish roles and responsibilities concerning electronic signature.
- To determine the electronic approval solutions according to the type of document to be signed.
- To standardize the methods used to electronically sign documents.

2. Scope

This Framework applies to documents *created and issued by* Concordia for electronic signature; It does not apply to documents *received* for signature.

3. Definitions

3.1. E-signature

An e-signature or electronic signature is a signature made electronically that has the same legal value as a handwritten signature. It includes a documented process and audit trail which has the same legal value as a handwritten signature.

3.2. Audit Trail

The audit trail is the evidence gathered during the electronic signature process, from the creation of the request to the obtaining of a signature. It maintains the link between the signatory and the document and ensures the integrity of the document (non-alteration of the document) and therefore the legal value of the e-signature. The audit trail is embedded as metadata in the electronically signed document.

4. Institutional e-signature solution

DocuSign is the institutional e-signature solution at Concordia. DocuSign provides an audit trail which ensures the integrity of documents.

5. Roles and responsibilities

5.1. IITS

- Responsible for technical management and configuration of e-signature solution.
- Provide technical support to e-signature issuers, as required.
- Ensure security controls for user authentication.
- Manage relationship with the e-signature solution provider.
- Ensure technical alignment with this Framework.
- Manage and maintain integration points with the e-signature solution.

5.2. Records Management and Archives (RMA)

- Develop and oversee e-signature framework and use of electronic signatures.
- Monitor usage to ensure proper development.
- Act as point of contact for units and departments.
- Act as point of contact for requests to assess alignment of the Framework with potential new opportunities.
- Analyze use cases and requirements, recommend signature types, and data classification. Submit to legal for approval, as required.
- Provide and configure secure sites within CONDOR, **Con**cordia's **Do**cument **R**epository.
- Ensure proper retention and destruction of electronically signed documents and their audit trails.
- Provide training and training material to end-users.

5.3. University Secretariat

- Provide legal advice on the use of e-signature processes.

5.4. Units and departments

- Ensure compliance with this Framework.
- Incorporate e-signature process into existing business processes, as needed.
- Use institutional e-signature solution, as required.
- Contact RMA to establish potential need for e-signature within a unit.

6. Types of approvals

DocuSign should be used primarily for documents listed in the *Policy on Contract Review, Signing and Required Approvals* (BD-1).

DocuSign does not automatically insert signatory information within documents. E-signature issuers must therefore consider the time and labour required to manually enter signatory contact information and the locations of signature lines. Therefore, email approvals will often be a more efficient alternative to e-signature.

Please contact RMA for assistance in choosing the best e-signature solution for your case: records.management@concordia.ca.

The following outlines the types of approvals at Concordia:

Description	Example	E-Signature Solution	Save location
1. Internal documents as part of manual processes.	Internal forms or documents: • Intake forms • Parking requests • Incident reports • Employee ID card requests • Etc.	Written approvals issued by a Concordia Email Account are sufficient. Approval documents should be attached and kept on file.	CONDORis recommended. Documents can also be saved in departmental drives.
2. Internal documents as part of workflows managed in information systems such as SIS, FRIS, SAP/Unity, etc.	• Expenses Reports • Notice of Hire, Notice of Change, Notice of Termination • Time sheets • Vacation requests • Etc.	Approvals via checkbox, approval button, etc. within institutional information systems.	Document repository within institutional information systems. If unavailable, use CONDOR.
3. Documents listed in the *Policy on Contract Review, Signing and Required Approvals* (BD-1).	• Agreements and Contracts • Leases • Letters of understanding • Etc.	DocuSign	CONDOR

7. E-Signature Procedure

7.1. Overview

a. DocuSign is the only electronic signature software which complies with this Framework and which is approved by the University Secretariat and IITS.
b. An e-signature request must be issued by the University and sent from an individual valid Concordia Email Account. Requests from role accounts (i.e. info@concordia.ca) and personal email accounts are invalid.
c. DocuSign shall be used to issue an electronic signature request for documents listed in the *Policy on Contract Review, Signing and Required Approvals* (BD-1).
d. Delegation of signatures is permitted as per *Policy on Contract Review, Signing and Required Approvals* (BD-1).
e. Scanned images of a handwritten signature do not constitute a valid e-signature unless used within DocuSign.
f. A self-signed certificate issued by Acrobat products does not constitute an e-signature. This type of certificate does not comply with this Framework because the integrity and authenticity of the documents is not preserved.
g. It is recommended to save electronically signed documents in CONDOR, in accordance with the *Records Classification and Retention Plan* (RCRP). Saving documents in online products not supported or approved by IITS, such as Google Drive or DropBox, is not permitted.
h. As with any other document, electronically signed documents are retained according to the retention policies set out in the RCRP, as required by the *Archives Act* (A-21.1).

7.2. E-signature Issuer

An e-signature issuer is the individual issuing an e-signature request. As with paper signatures, the signature issuer is responsible for:

- Sending the e-signature request to the signatory's individual email address. These requests should not be sent to group or role accounts, i.e., info@concordia.ca.
- Authenticating the signatory by ensuring the contact information originates from a trusted source such as an institutional information system, or directly by email or telephone.
- Ensuring the correct version of the document is sent to the signatory.
- Monitoring the progress of an electronic signature request.
- Responding to questions from the signatory during the signature process.
- Saving the electronically signed document in CONDOR.

7.3. DocuSign Settings

- The signatory is required to sign documents within no more than **10 days** of receiving an e-signature request. Both the signatory and the issuer have access to the document during the **10-day** signing period.
- The issuer and the signatory have access to the electronically signed document in DocuSign for **30 days** following the signing. Both the issuer and the signatory can access and download the document during the **30-day** period.
- Electronically signed documents are kept in DocuSign for **30 days** following the signing. The issuer should save them in CONDOR within **30 days** of the signing.

8. E-signature Workflow