Document Retention Policy

Version 1.0
January 1, 2023

This Policy is confidential and for the use of enVista associates only. Do not distribute this document externally.

enVista®
enabling enterprise commerce™

I. Reasons for Policy

enVista, LLC (“enVista”) and its affiliates possess vital business records, data, and information regarding its operations and those of its clients in order to conduct its business. Federal, state, and international laws and regulation requires enVista to retain certain enVista and third party business records, data and information only for a specific amount of time. Accordingly, enVista has adopted this Document Retention Policy and Record Retention Schedule attached hereto (the “Policy”) to govern enVista’s retention and destruction of business records, data and information, regardless of the format.

The accidental or intentional destruction of these records during their specified retention periods set forth in the appendix to this Policy could result in the following consequences for enVista and/or its associates:

- Fines and penalties.
- Loss of rights.
- Obstruction of justice charges.
- Inference of spoliation of evidence and spoliation tort claims.
- Contempt of court charges.
- Serious disadvantages in litigation.

enVista must retain certain records because they contain information that:

- Serves as enVista's corporate memory.
- Has enduring business value (for example, it provides a record of a business transaction, evidences enVista's rights or obligations, protects enVista's legal interests or ensures operational continuity).
- Must be kept to satisfy legal, accounting, employer or other regulatory requirements.

enVista prohibits the inappropriate destruction of any records, files, documents, samples, and other forms of information in breach of this Policy. Therefore, this Policy is part of a company-wide system for the review, retention, and destruction of records enVista creates or receives in connection with the business it conducts.

II. Types of Documents

This Policy explains the differences among records, disposable information, and confidential information belonging to others.

III. Records

A record is any type of information created, received, or transmitted in the transaction of enVista's business, regardless of physical format. Examples of where the various types of information are located include:

- Audio and video recordings.
- Calendars.
- Computer programs.
- Contracts.

- Electronic files.
- Emails.
- Handwritten notes.
- Invoices.
- Letters and other correspondence.
- Online enVista sponsored postings, such as on Facebook, Twitter, Instagram, Snapchat, Slack, Reddit, Vine, and other social media platforms and websites.
- Performance reviews.
- Voicemails.

Any file that is listed in the Records Retention Schedule contained in the Appendix to this Policy, must be retained for the amount of time indicated in the Records Retention Schedule or longer if subject to a litigation hold, as described below. The retention period set forth in the Appendix as it applies to personal information may be for a shorter period of time, if required by law as requested by an individual. A record must not be retained beyond the period indicated in the Record Retention Schedule, unless a valid business reason (or a litigation hold or other special situation) calls for its continued retention. If you are unsure whether to retain a certain record, contact the Legal Department.

IV. Disposable Information

Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a record as defined by this Policy or subject to a litigation hold as described below. Examples of disposable information may include:

- Duplicates of originals that have not been annotated.
- Preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record.
- Books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of enVista and retained primarily for reference purposes.
- Spam and junk mail.

V. Confidential Information Belonging to Others

Any confidential information that an associate may have obtained from a source outside of enVista, such as a previous employer, must not, so long as such information remains confidential, be disclosed to or used in conjunction with an associate’s scope of employment with enVista. Unsolicited confidential information submitted to enVista should be refused, returned to the sender where possible, and deleted.

VI. Mandatory Compliance

A. **Responsibility of All Associates** enVista strives to comply with the applicable laws, rules, and regulations that govern it and with recognized compliance practices. All company associates must comply with this Policy, the Records Retention Schedule and any litigation hold communications. Failure to do so may subject enVista, its associates, and contract staff to serious civil and/or criminal liability. An associate's failure to comply with this Policy may result in disciplinary sanctions, including suspension or termination.

B. Reporting Policy Violations

enVista is committed to enforcing this Policy as it applies to all forms of records. The effectiveness of enVista's efforts, however, depends largely on associates. If you feel that you or someone else may have violated this Policy, you should report the incident immediately to your supervisor. If you are not comfortable bringing the matter up with your immediate supervisor, or do not believe the supervisor has dealt with the matter properly, you should immediately raise the matter with enVista's General Counsel. If associates do not report inappropriate conduct or violations of this Policy, enVista may not become aware of a possible violation of this Policy and may not be able to take appropriate corrective action. No one will be subject to and enVista prohibits, any form of discipline, reprisal, intimidation, or retaliation for reporting incidents of inappropriate conduct of any kind, pursuing any record destruction claim, or cooperating in related investigations.

VII. Records Management Process

The Records Management Committee, appointed from time to time by the enVista Executive Leadership Team ("ELT"), is responsible for the initial implementation and ongoing monitoring of this Policy. The Records Management Committee will identify the documents that enVista must or should retain, and determining, in collaboration with the Legal Department, and the proper period of retention of such documents. Members of the Records Management Committee may include the enVista General Counsel, Security Leader, Manager of Information Technology, and . Other roles may be added from time to time. The Records Management Committee has identified the documents that enVista must or should retain, and determined the proper period of retention and oversees the proper storage and retrieval of records, coordinating with outside vendors where appropriate. The Records Management Committee's designee(s) will arrange for the proper storage and retrieval of records, coordinating with outside vendors where appropriate. Additionally, the Records Management Committee's designee handles the destruction of records whose retention period has expired.

The Records Management Committee is responsible for:

- Administering the Records Management program and helping department heads implement it and related best practices.
- Planning, developing, and prescribing document disposal policies, systems, standards, and procedures.
- Writing straightforward document management procedures to instruct employees on how to comply with this Policy.
- Monitoring departmental compliance so that employees know how to follow the document management procedures and the Legal Department has confidence that enVista's records are controlled.
- Ensuring that senior management is aware of their departments' document management responsibilities.
- Developing and implementing measures to ensure that the Legal Department knows what information enVista has and where it is stored, that only authorized users have access to the information, and that enVista keeps only the information it needs, thereby efficiently using space.

- In cooperation with department heads, identifying essential records and establishing a disaster recovery plan for each office and department to ensure maximum availability of enVista's records in order to reestablish operations quickly and with minimal interruption and expense.
- Developing procedures to ensure the permanent preservation of enVista's historically valuable records.
- Providing document management advice and assistance to all departments by preparing manuals of procedure and Policy and by on-site consultation.
- Determining the practicability of and, if appropriate, establishing a uniform filing system and a forms design and control system.
- Periodically reviewing the records retention schedules and administrative rules issued by the applicable countries to determine if enVista's document management program and its Records Retention Schedule is in compliance with state and foreign regulations.
- Distributing to the various department heads information concerning state laws and administrative rules relating to corporate records.
- Explaining to employees their duties relating to the document management program.
- Ensuring that the maintenance, preservation, microfilming, computer disk storage, destruction, or other disposition of enVista's records is carried out in accordance with this Policy, the procedures of the document management program and the requirements of federal and state law.
- Planning the timetable for the annual records destruction exercise and the annual records audit, including setting deadlines for responses from departmental staff.
- Maintaining records on the volume of records destroyed under the Records Retention Schedule and the records stored electronically.
- Evaluating the overall effectiveness of the document management program.
- Reporting annually to the Legal Department on the implementation of the document management program in each of enVista's departments.
- Bringing to the attention of the Legal Department any noncompliance by department heads or other employees with this Policy and enVista's document management program.

How to Store and Destroy Records

Storage enVista's records must be stored in a safe, secure, and accessible manner. Any documents and financial files that are essential to enVista's business operations during an emergency must be duplicated and/or backed up at least once per week and maintained in a segregated location.

Destruction enVista's executive officer overseeing the particular category of record is responsible for the continuing process of identifying the records that have met their required retention period and supervising their destruction. The destruction of confidential, financial, and personnel-related records must be conducted by shredding if possible. Non-confidential records may be destroyed by recycling. The destruction of electronic records must be coordinated with the IT Department manager.

The destruction of records must stop immediately upon notification from the Legal Department that a litigation hold is to begin because enVista is or may be involved in a lawsuit or an official investigation (see next paragraph). Destruction may begin again once the Legal Department lifts the relevant litigation hold.

Litigation Holds and Other Special Situations

enVista requires all associates to comply fully with its published records retention schedule and procedures as provided in this Policy. All associates should note the following general exception to any stated destruction schedule:

> **If you believe or the Legal Department informs you that enVista records are relevant to current litigation, potential litigation (that is, a dispute that could result in litigation), government investigation, audit, or other event, you must preserve and not delete, dispose, destroy, or change those records, including emails, until the Legal Department determines those records are no longer needed. This exception is referred to as a litigation hold or legal hold, replaces any previously or subsequently established destruction schedule for those records. If you believe this exception may apply, or have any questions regarding whether it may possibly apply, please contact the Legal Department.**

In addition, you may be asked to suspend any routine document disposal procedures in connection with certain other types of events, such as the merger of enVista with another organization or the replacement of one or more enVista information technology systems.

Audits and Associate Questions

Internal Review and Policy Audits The Chief Executive Officer and General Counsel of enVista will periodically review this Policy and its procedures with to ensure enVista is in full compliance with relevant new or amended regulations and laws. Additionally, enVista may audit associate files and computer hard drives to ensure compliance with this Policy.

Questions About the Policy Any questions about this Policy should be referred to Amy L. Mader, Esq. amader@envistacorp.com who is in charge of administering, enforcing, and updating this Policy.

APPENDIX

Record Retention Schedule

To the enVista, LLC

Document Retention Policy

enVista, LLC establishes the retention or destruction schedules or procedures for specific categories of records, as set forth below and subject to the Document Retention Policy. This is done to ensure legal compliance and accomplish other objectives, such as protecting intellectual property and controlling costs. Associates should give special consideration to the categories of documents listed in the record retention schedule below. Avoid retaining a record if there is no business reason for doing so and consult with the Legal Department if unsure.

RECORD, IF APPLICABLE	RETENTION PERIOD MINIMUMS*
Personnel Records	
Benefits descriptions per associate	4 years
EEO-1 Reports (Employer Information Report)	Filed annually with the EEOC and the Department of Labor, Office of Federal Contract Compliance Programs, most recent kept on file
Associate applications and resumes	4 years
Associate benefit plans subject to ERISA (includes plans regarding health and dental insurance, 401K, long-term disability, and Form 5500)	6 years from when the record was required to be disclosed. Full period the plan or system is in effect and at least 1 year after termination of plan
Associate offer letters (and other documentation regarding hiring, promotion, demotion, transfer, lay-off, termination or selection for training)	1 year from date of making record or action involved, whichever is later, or 1 year from date of involuntary termination
Records relating to background checks on associates	5 years from when the background check is conducted
Employment contracts; employment and termination agreements	3 years from an associate's termination
Associate records with information on pay rate or weekly compensation	3 years
Hazardous material exposures	Duration of employment + 30 years
I-9 Forms	3 years after date of hire or 1 year after employment is terminated, whichever is later/3 years after date of hire
Injury and Illness Incident Reports (OSHA Form 301) and related Annual Summaries (OSHA Form 300A); Logs of work-related injuries and illnesses (OSHA Form 300)	5 years following the end of the calendar year that these records cover

Supplemental record for each occupational injury or illness (OSHA Form 101); Log and Summary of Occupational Injuries and Illnesses (OSHA Form 200)	5 years following the year to which they relate
Job descriptions, performance goals and reviews; garnishment records	3 years after termination
Associate tax records	4 years from the date tax is due or paid
Personnel or employment records	3 years from the date the record was made or personnel action was taken, whichever is later
Pension plan and retirement records	Permanent
Salary schedules; ranges for each job description	3 years
Time reports	Termination + 3 years
Workers' compensation records	Duration of employment + 30 years
Written affirmative action program (AAP) and supporting documents	For immediately preceding AAP year, unless it was not then covered by the AAP year
Payroll Records	
Payroll records (pay rate, earnings records, additions to or deductions from wages)	3 years from the last date of entry
W-2 and W-4 Forms and Statements	As long as the document is in effect + 4 years
Corporate Records	
Articles of Incorporation, Bylaws, Corporate Seal	Permanent
Annual corporate filings and reports to secretary of state and attorney general	Permanent
Board policies, resolutions, meeting minutes, and committee meeting minutes	Permanent
Contracts	Permanent if current (7 years if expired)
Construction documents	Permanent
Emails (business related)	3 years
Fixed Asset Records	Permanent
IRS Form 1023 (Application for charitable and/or tax-exempt status)	Permanent
IRS Determination Letter	Permanent
Sales and purchase records	3 years
State sales tax exemption documents	Permanent
Resolutions	Permanent
Client Records & Information	
List of clients	7 years from date of disengagement
Client complaints; compensation records	3 years

Client data	Subject to applicable law and Client agreements. Project plans and equipment specifications held by the Automation Solution Group.
Tax Records	
Annual tax filing for the organization (IRS Form 990 in the US)	Permanent
Filings of fees paid to professionals (IRS Form 1099 in the US)	7 years
Payroll tax withholdings	7 years
Earnings records	7 years
Payroll tax returns	7 years
State unemployment tax records	Permanent
Legal and Insurance Records	
Appraisals	Permanent
Copyright registrations	Permanent
Environmental studies	Permanent
Insurance claims/ applications	Permanent
Insurance disbursements and denials	Permanent
Insurance contracts and policies (Directors and Officers, General Liability, Property, Workers' Compensation)	Permanent
Leases	6 years after expiration
Patents, patent applications, supporting documents	Permanent
Real estate documents (including loan and mortgage contracts, deeds)	Permanent
Stock and bond records	Permanent
Trademark registrations, evidence of use documents	Permanent
Warranties	Duration of warranty + 7 years

Accounting and Finance	
Accounts Payable and Receivables ledgers and schedules	3 years
Annual audit reports and financial statements	Permanent
Annual plans and budgets	3 years
Bank statements, cancelled checks, deposit slips	7 years

Business expense records	3 years
Cash receipts	3 years
Check registers	Permanent
Electronic fund transfer documents	3 years
Associate expense reports	3 years
General ledgers	Permanent
Journal entries	3 years
Invoices	3 years
Petty cash vouchers	3 years

Associate Communications	
Business Emails	3 years* *IRS communications need to be kept for 7 years; state tax communications need to be retained for 3 years. *HIPAA: Communications retained for 6 years. *Executive communications shall be retained for longer periods at the discretion of the Records Management Committee.
Microsoft Teams Private Chats	180 days
Microsoft Teams Channel Communications	365 days
Email Address Removal	6 months for all associates, except ELT members and sales. ELT and sales associates will be held for 12 months.
Zoom recordings pulled from Zoom.	365 for enVision and enForm corporate meetings 90 days for all other meetings

Client & Project Documents	
Project Documents (i.e. technical design documents, project sites)	3 years
Personal Information accessed in conjunction with Client & Project Documents	Dispose once the Personal Information is no longer needed for enVista to perform its services.

Client Relationship Management System	5 years from last invoice date.
Microsoft Teams / SharePoint Sites (projects)	3 years after project completion
Microsoft Teams / SharePoint Sites (non-projects)	1 year

Information Technology Management Records	
Infrastructure and System Project Records	5 years after system / version has been superseded
Information technology operations and maintenance records	3 years after control has completed
Configuration and change management records	5 years after no longer needed
Information technology oversight and compliance records	5 years after no longer needed

Information Systems Security Records	
Systems and data security records	1 year after superseded
Computer Security Incident handling, reporting and follow-up records (Security Incident means a violation or imminent threat of violation of enVista cybersecurity policies, acceptable use policies, or standard security practices).	1 year after completion
System access records	Destroy after business use no longer needed Special access accounts and associated records: 6 years

Information Technology Administrative Management and Oversight Records	
Technology audits, examinations, internal control reviews, investigations, responses, and mitigation management documents	5 years after conclusion of the activity
Policy, Standards, and Guidelines	Maintain 1 version back