	Policy: Document Retention Policy
	Revision Level Date: Rev. 0- 02/16/2023
	Department: Legal
	Page 1 of 10

REVISION HISTORY

REVISION LEVEL/DATE	DESCRIPTION
Rev. 0- 02/16/2023	Initial Release

I. Purpose and Scope

The purpose of this Document Retention Policy (this “Policy”) is to establish the procedures for the retention and destruction of corporate records, files, emails, documents, intellectual property, and other information, and applies to Workhorse Group Inc. and each of its subsidiaries (collectively, the “Company”). The Company prohibits the inappropriate or unlawful destruction of, or tampering with any records, files, documents, samples, and other forms of information. Therefore, this Policy is part of a Company-wide system for the review, retention, and destruction of records the Company creates or receives in connection with the business it conducts.


The Company strives to comply with the laws, rules, and regulations that govern it and with recognized compliance practices. It is the responsibility of all Company employees to comply with this Policy, the Records Retention Schedule, and any litigation hold communications or other notices from the Legal Department or its designee regarding retention of records. Failure to do so may subject the Company, its employees, and contract workers to serious civil and/or criminal liability. An employee’s failure to comply with the letter and/or spirit this Policy may result in disciplinary sanctions, including, but not limited to, suspension or termination.

Federal and state laws require the Company to retain certain records for a specific amount of time. The Sarbanes-Oxley Act of 2002 establishes that it is a crime to change, conceal, falsify, or destroy any record with the intent to impede or obstruct any official or government proceeding. The accidental or intentional destruction of these records during their specified retention periods could result in the following consequences for the Company and/or its employees:

- 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.

In addition, certain records must be retained by the Company because they contain information that:

- Serves as the Company’s corporate memory.

	Policy: Document Retention Policy
	Revision Level Date: Rev. 0- 02/16/2023
	Department: Legal
	Page 1 of 10

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


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

II. Types of Documents

Records. A record is any type of information created, received, or transmitted in the transaction of the Company's business or prospective business opportunities, regardless of physical format. Records may be located in:

- Appointment books and calendars.
- Audio and video recordings.
- Computer programs.
- Contracts.
- Electronic files.
- Emails.
- Engineering drawings and design specifications.
- Handwritten notes.
- Invoices.
- Letters and other correspondence.
- Cell phone data.
- Company online postings, such as on Facebook, Twitter, Instagram, Snapchat, Slack, Reddit, TikTok, YouTube, and other social media platforms and websites.
- Performance reviews.
- Test samples and data.
- Voicemails.
- Personnel files.
- Payroll systems.

Therefore, any paper records and electronic files that are part of any of the categories 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, regardless of medium. 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 identified and/or confirmed by the Legal Department or its designee) calls for its continued retention. If you are unsure whether to retain a certain record, contact the Chief Compliance Officer or a member of the Legal Department.

	Policy: Document Retention Policy
	Revision Level Date: Rev. 0- 02/16/2023
	Department: Legal
	Page 1 of 10

Disposable Information. Disposable information consists of data that may be discarded or deleted (as set forth in the “Destruction” section below) 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. Examples 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 the Company and retained primarily for reference purposes.
- Spam and junk mail or email.

Email. The contents of an email message and any accompanying attachments may include other records, and the specific record retention requirements for that type of record apply to the contents of email messages. It should be noted that **Email is not an acceptable record storage system**, and that all records should be stored in the Company’s SharePoint or other approved secured server and not in an employee’s email account alone. Contracts and other documents, including those signed through email communication, should be sent to the Legal Department promptly upon execution of those documents. The use of personal email accounts for Company business is prohibited.

It is the Company’s policy to regularly delete emails of former employees after 3 years. Supervisors are instructed to clean out the email accounts of departing employees. Company email accounts are considered property of the Company, and employees have no right of privacy as to any information or file maintained in or on Company property or transmitted or stored through Company computer systems. For more information, refer to the Company’s Computer Use Policy and Use of Company Assets Policy.

Confidential Information Belonging to Others. Any confidential information that an employee may have obtained from a source outside of the Company, such as a previous employer, must not, so long as such information remains confidential, be disclosed to or used by the Company (including, but not limited to, use by the employee in the course of or for the benefit of the Company). Unsolicited confidential information submitted to the Company should be refused, returned to the sender where possible, and deleted, if received via the internet.

Confidential information belonging to other companies may be subject to a nondisclosure agreement or other legal document that requires the return or destruction of such information at a specified time. Confidential information belonging to other companies and obtained by or otherwise disclosed to an employee or the Company in the course of and in furtherance of an actual or prospective business relationship with the Company may be used and/or disclosed only to the extent permitted by any applicable non-disclosure agreement or other agreement and only to the extent permitted by law, and necessary for the employee to perform their job duties

	Policy: Document Retention Policy
	Revision Level Date: Rev. 0- 02/16/2023
	Department: Legal
	Page 1 of 10

for the Company. If you are unsure whether to retain confidential information belonging to other companies, contact the Chief Compliance Officer or a member of the Legal Department.

Employees are hereby advised that the Defend Trade Secrets Act of 2016 provides immunity from civil and criminal liability under state and federal trade secret laws for any employee who discloses a trade secret in a lawsuit or other proceeding filed under seal or who discloses a trade secret in confidence to a government official or an attorney for the sole purpose of reporting or investigating a suspected violation of law.

Lastly, Confidential Information may also include personally identifiable information of employees, customers, or third parties that might also be subject to regulatory requirements for retention, deletion or portability. Accordingly, the Company may implement additional requirements for such actions taken under applicable law.

III. Reporting Policy Violations


The Company is committed to enforcing this Policy as it applies to all forms of records. The effectiveness of the Company's efforts, however, depends largely on employees. If you have seen, heard about, or otherwise been made aware of a potential violation of 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 raise the matter with the Chief Compliance Officer. If employees do not report inappropriate conduct, the Company may not become aware of a possible violation of this Policy and may not be able to take appropriate corrective action. Upon receiving a report of a potential violation of this Policy, the Company or its designee will promptly and thoroughly investigate the matter and the Company will take appropriate corrective action. Employees are required, as a condition of their employment, to participate in good faith in any such investigation.

No one will be subject to and the Company prohibits, any form of discipline, reprisal, intimidation, or retaliation for reporting incidents in good faith that may constitute a violation of this Policy, pursuing any charge, claim, or other cause of action related to record retention and destruction requirements or this Policy, or cooperating in good faith in related investigations or proceedings. For further information, see the Company's Whistleblower Policy.


IV. Legal Department and Chief Compliance Officer

The Legal Department is responsible for identifying the documents that the Company must or should retain, and determining, in collaboration with the Director of Internal Audit, the proper period of retention. It also arranges for the proper storage and retrieval of records, coordinating with outside vendors where appropriate.

The Chief Compliance Officer is responsible for:

	Policy: Document Retention Policy
	Revision Level Date: Rev. 0- 02/16/2023
	Department: Legal
	Page 1 of 10

- Administering the document 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 the Company'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 the Company has and where it is stored, that only authorized users have access to the information, and that the Company keeps only the information it needs, thereby efficiently using space.
- Establishing standards for filing and storage equipment and recordkeeping supplies.
- In cooperation with department heads, identifying essential records and establishing a disaster plan for each office and department to ensure maximum availability of the Company's records in order to reestablish operations quickly and with minimal interruption and expense.
- Developing procedures to ensure the permanent preservation of the Company'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 governments of Ohio, Indiana, Michigan, Delaware, and Nevada to determine if the Company's document management program and its Records Retention Schedule is in compliance with state regulations.
- Explaining to employees their duties relating to the document management program.
- Planning the timetable for the annual records destruction exercise and the annual records audit, including setting deadlines for responses from departmental staff.
- Evaluating the overall effectiveness of the document management program.
- Reporting annually to the Board of Directors on the implementation of the document management program.

	Policy: Document Retention Policy
	Revision Level Date: Rev. 0- 02/16/2023
	Department: Legal
	Page 1 of 10

V. How to Store and Destroy Records

Storage. The Company's records must be stored in a safe, secure, and accessible manner (to those with a business reason to access the records). Any documents and financial files that are essential to the Company's business operations during an emergency must be backed up and maintained. Essential physical records should be saved in digital format, and any essential information stored on the Company SharePoint must also be backed up on a secured server. Access to the Company's records (in any format, including hard copy or electronic copy) must be limited to those with authorization and a business need to access such records; this includes, but is not limited to, limiting access to such records by use of lock and key, password, or other means of exclusion (note, the Company's records are the property of the Company, and the Company retains the right, among others, to access any and all Company records of any nature including, but not limited to, records that are protected by lock and key, password, or other means of exclusion; employees have no expectation of privacy in relation to the Company's property, the presence of the employee or the employee's personal property on Company premises, the employee's use of Company's systems, or otherwise in the course of employment with the Company).


Destruction. The Company's Chief Compliance Officer 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. Once the applicable retention period has concluded, non-confidential records may be destroyed by recycling. The destruction of electronic records must be coordinated with the Director of IT.

To aid in the regular destruction of records that have exceeded the required retention period, the Company will implement a regular document destruction period on at least an annual basis for both electronic and physical documents. The Chief Compliance Officer is responsible for this process, which will be coordinated with the Director of IT.

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

VI. Litigation Holds and Other Special Situations

The Company requires all employees to comply fully with its published records retention schedule and procedures as provided in this Policy. All employees should note the following general exception to any stated destruction schedule: If you believe, or the Legal Department informs you, that the Company records are or may be 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,

	Policy: Document Retention Policy
	Revision Level Date: Rev. 0- 02/16/2023
	Department: Legal
	Page 1 of 10


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, and 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, you must immediately 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 the Company with another organization or the replacement of the Company's information technology systems.

VII. Audits and Employee Questions

Internal Review and Policy Audits. The Director of Internal Audit and the General Counsel of the Company will periodically review this Policy and its procedures with outside legal counsel and the Company's certified public accountants to ensure the Company is in full compliance with relevant new or amended regulations. Additionally, the Company may regularly audit employee files and computer hard drives to ensure compliance with this Policy. Employees will be asked to acknowledge this policy following any major changes.

Questions About the Policy. Any questions about this Policy should be referred to the Chief Compliance Officer, who is in charge of administering, enforcing, and updating this Policy.

	Policy: Document Retention Policy
	Revision Level Date: Rev. 0- 02/16/2023
	Department: Legal
	Page 1 of 10

APPENDIX

Record Retention Schedule

Occasionally the Company establishes retention or destruction schedules or procedures for specific categories of records. This is done to ensure legal compliance and accomplish other objectives, such as protecting intellectual property and controlling costs. Employees 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 Chief Compliance Officer or Legal Department if unsure.

RECORD	RETENTION PERIOD
Personnel Records	
Benefits descriptions per employee	8 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
Employee applications and resumes	4 years
Employee benefit plans subject to ERISA (includes plans regarding health and dental insurance, 401K, long-term disability, and Form 5500)	8 years from when the record was required to be disclosed
Employee 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 employees	5 years from when the background check is conducted
Employment contracts; employment and termination agreements	8 years from their last effective date
Employee records with information on pay rate or weekly compensation	3 years
I-9 Forms	3 years after date of hire or 1 year after employment is terminated, whichever is later
Job descriptions, performance goals and reviews; garnishment records	Termination + 7 years
Employee tax records	4 years from the date tax is due or paid
Medical exams required by law	Duration of employment + 30 years
Personnel or employment records	2 years from the date the record was made or personnel action was taken, whichever is later




Policy: Document Retention Policy

Revision Level Date: Rev. 0- 02/16/2023

Department: Legal

Page 1 of 10

Pension plan and retirement records	Permanent
Pre-employment tests and test results	1 year from date of personnel action
Salary schedules; ranges for each job description	2 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
Emails (business related)	3 years
Safety Records	
Fire and extinguisher safety and maintenance records	Until the extinguisher is taken out of service.
Certification record of inspections of mechanical power presses, the clutch/brake mechanism, anti-repeat feature, and single stroke mechanism	Until the mechanism is replaced
Hazardous material exposure records and analyses	Duration of employment + 30 years
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
Certification records of employee training for mechanical equipment and vehicle operation	Duration of employment
Certification records of employee safety-related work practices and procedures training	Duration of employment
Documentary materials, films, tapes, and other information-storing media that contain information concerning malfunctions that may be related to motor vehicle safety including electronic records and internal or external communications pursuant to NHTSA Record Retention requirements. 49 CFR Part 576	5 years from the date of generation or acquiring of records by the manufacturer.
Payroll Records	
Payroll registers (gross and net)	3 years from the last date of entry

	Policy: Document Retention Policy
	Revision Level Date: Rev. 0- 02/16/2023
	Department: Legal
	Page 1 of 10

Federal procurement contract and related weekly payroll documents	4 years from completion of contract
Time cards; piece work tickets; wage rate tables; pay rates; work and time schedules; earnings records; records of additions to or deductions from wages; records on which wage computations are based	2 years
W-2 and W-4 Forms and Statements	As long as the document is in effect + 4 years
Engineering and Technical Data	
Records relevant to an ongoing design or project, including design drawings and specifications, test samples,	Permanent if current
Records relevant to an abandoned design or project	3 years
Patents, patent applications, supporting documents	Permanent
Documentary materials, films, tapes, and other information-storing media that contain information concerning malfunctions that may be related to motor vehicle safety including electronic records and internal or external communications pursuant to NHTSA Record Retention requirements. 49 CFR Part 576	5 years from the date of generation or acquiring of records by the manufacturer.
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 Determination Letter	Permanent
Sales and purchase records	3 years
State sales tax exemption documents	Permanent
Resolutions	Permanent
Securities Records	




Policy: Document Retention Policy

Revision Level Date: Rev. 0- 02/16/2023

Department: Legal

Page 1 of 10

Audit and review workpapers	5 years from the end of the fiscal period in which the audit or review was concluded
Documents supporting management's assessment of internal controls over financial reporting	Permanent
List of clients that are covered associates and government entities	5 years
Original signature pages or other documents showing the signatures of certifying officers in SEC filings	5 years from date of filing
Records relevant to an audit or review, including memoranda, correspondence and other communications	7 years after conclusion of audit or review
Accounting and Finance	
Accounts Payable and Receivables ledgers and schedules	7 years
Annual audit reports and financial statements	Permanent
Annual plans and budgets	2 years
Bank statements, cancelled checks, deposit slips	7 years
Business expense records	7 years
Cash receipts	3 years
Check registers	Permanent
Electronic fund transfer documents	7 years
Employee expense reports	7 years
General ledgers	Permanent
Journal entries	7 years
Invoices	7 years
Petty cash vouchers	3 years
Tax Records	
Annual tax filing for the organization (IRS Form 1120 in the US)	7 years
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

	Policy: Document Retention Policy
	Revision Level Date: Rev. 0- 02/16/2023
	Department: Legal
	Page 1 of 10

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