US LBM Holdings, LLC

Data and Record Management, Retention and Storage Policy

PEOPLE

PARTNERSHIPS

OPERATIONAL EXCELLENCE

CONTINUOUS IMPROVEMENT

EMPOWERMENT

Purposes

US LBM Holdings, LLC ("**US LBM**"), together with its subsidiary operating companies ("**Divisions**" and collectively the "**Company**"), is committed to ensuring that (1) certain information received by the Company is appropriately managed and maintained in compliance with all legal and regulatory requirements, (2) records and documents of the Company are adequately protected and maintained, and (3) documents and information which are no longer needed by the Company or are of no value are properly destroyed at the right time. This Policy is also for the purpose of assisting associates and consultants of the Company in understanding their obligations in managing, retaining and storing data and records. Following this Policy will also allow the Company to save money and time and operate more efficiently.

Scope

This Policy covers: (a) retention, storage and maintenance of Data and Records (defined below), which is necessary for the functioning of the Company and to comply with legal and regulatory requirements, and (b) the destruction of Data and Records which no longer need to be retained.

It is the responsibility of all associates to comply with this Policy. Failure to adhere to this Policy may result in disciplinary action up to and including termination of employment, and/or personal civil and criminal liability.

Key Definitions

The term "**Data**" includes any information which is processed or stored by or on behalf of the Company, including hard copy and electronic information. Data may be processed, handled, managed, or stored internally by an associate or externally by a subcontractor, vendor, or other party on the Company's behalf. Data may include information regarding our associates, customers and others we do business with.

The term "**Personal Data**" means any information that relates to a person or household who could be identified with that information (this includes indirect or inferred identification, i.e. a Social Security Number may not on its face identify a person, but with some homework that person could eventually be identified). If you have any questions about what is and is not Personal Data, please contact the legal department.

The term "**Record**" applies to all documents, both paper and electronic (including e-mails and instant messages), created or received by the Company which relate to company business and which should be preserved because it has business value or legal significance. Records are the property of the Company and an associate has no personal or property right to Records, including those Records the associate helped develop or write.

Examples of Records include paper or electronic files, correspondence and communications that:

- Document an event or activity related to business.
- Demonstrate a business transaction.
- Identify individuals who participated in a business activity.
- Support facts of an event, activity, or transaction related to the business.
- Are needed for legal, business, or compliance reasons, such as being relevant to a pending or anticipated lawsuit or audit.

All documents which do not fall within the meaning of Records will be considered "**Non-Records"** and should be deleted or disposed of when they no longer have business value. Examples of Non-Records include:

- General company-wide or department announcements, notices or updates.
- Duplicates of originals which do not contain unique notes.
- Preliminary drafts of letters, memoranda, reports, worksheets, and informal notes which do not represent significant steps or decisions in the preparation of an official Record.
- Books, periodicals, manuals, training binders, and other materials obtained from sources outside of the Company and retained primarily for reference purposes.
- Spam and junk mail or email.

The term "**CIO"** means the Chief Information Officer or his or her designee.

Roles and Responsibilities

Board of Directors (the "Board").

The Board maintains the ultimate responsibility for the Company's compliance with all applicable laws, regulations and regulatory guidance, as well as the requirements in this Policy.

The CIO

The CIO is responsible for:

- Owning, maintaining and enforcing this Policy and will report to executive management and to the Board regarding this Policy;
- Reviewing and acting on any requests for exceptions to the requirements of this Policy; and
- Making modifications to this Policy and/or the Record Retention Schedule from time to time to ensure compliance with applicable legal and regulatory requirements.

Corporate Departments and Division Management.

Each Corporate Department (i.e. Operations, Development, Finance, Culture, etc.) and all Division Management is accountable for the implementation, oversight and management of controls, processes, and procedures to drive compliance with this Policy and related laws and regulations. Specifically, each Corporate Department and all Division Management must:

- Establish and implement procedures and controls as necessary that clearly reflect the requirements of this Policy and which define roles and responsibilities;
- Act upon any breaches of this Policy by promptly reporting the matter to the CIO as soon as possible, and ensure ongoing compliance;
- Communicate to the CIO any changes to the Data being handled by their respective department, including new proposed Data streams or Data being sent to new third parties;
- Ensure that associates with responsibility for any aspect of compliance with this Policy are trained appropriately to meet their obligations;
- Establish retention and deletion timelines based on the Record Retention Schedule and adhere to those timelines for Data and Records as appropriate for their department in accordance with this Policy; and
- Ensure results of ongoing monitoring or risk and compliance initiatives are escalated to the CIO as necessary.

Data and Record Retention; Record Retention Schedule

There is no fixed period for which we should retain Data, meaning the retention period will be determined by other factors, including whether the Data is part of a Record listed under Appendix A. However, data protection laws that apply to the Company's business may require that we do not keep Personal Data in a form which permits identification of a person for any longer than is necessary for the purposes for which the Personal Data was collected. Consequently, it is important to retain Personal Data which is contained in Records for the retention period listed under Appendix A, and it is important to delete Personal Data once the Personal Data is no longer needed for the purposes for which it was collected and so long as Personal Data is not contained in a Record listed under Appendix A.

Appendix A of this Policy is a Record Retention Schedule which contains required time periods for the retention and disposal of Company Records. All associates, subcontractors, and consultants of the Company must comply with the Record Retention Schedule and are encouraged to revisit the most current version of the Record Retention Schedule to ensure continued compliance.

Maintenance and Storage of Records

Hard-Copy Records. Hard-copy Records, such as paper files, which contain confidential or sensitive information, including trade secrets, should always be stored in a secured space with physical access controls, such as a locked file cabinet, so that they are only accessible to associates and authorized personnel who have a legitimate business need to access such Records.

Electronic Records. Records should be stored securely in digital format where possible. Electronic Records may only be stored in Company-approved locations as defined by IT, such as Sharepoint, OneDrive, company databases, or company file shares. Email and instant messaging systems should not be used as a main storage site for Records and associates are responsible for storing Records which need to be maintained longer than twelve months outside of Email. Instant messages in particular should not be used to communicate or memorialize important company information (in other words, associates should avoid creating Records on an instant-messaging system). Electronic Records may not be stored on any computers or mobile devices not owned by the Company, such as an associate's personal laptop. Electronic Records may not be stored on any personal drives not under the

Company's control, such as a personal Google drive account. Associates should take care not to create duplicate Records in multiple files or locations, since the Company is striving to limit excess Records.

Records Destruction

When destroying Records under this Policy, we must always take care to protect the Company's Confidential Information and trade secrets. Physical Records should always be shredded before disposal and digital Records should be deleted fully, including any old versions or copies. In some cases, merely deleting a digital Record will not be sufficient. For more information on deleting Records in electronic form, see "Data Review and Destruction," below.

Data Management

Data Categories

To properly manage the Data we handle, the Data must be evaluated and identified as belonging to a certain category so that those who access the Data can know what levels of restrictions and controls apply. This applies to all Data, whether processed, handled, managed, or stored internally by an associate or externally by a subcontractor, vendor, or other party on the Company's behalf. Each associate is responsible for evaluating and identifying the Data's sensitivity and appropriate category in accordance with this Policy.

We use two levels of Data categories: (i) Sensitive Data and (ii) Non-Sensitive Data.

Sensitive Data. Sensitive Data includes any information determined to be confidential under law, under a contract, or deemed sensitive or confidential by the Company. It is the Company's policy that we only collect, use, and transmit the minimum amount of Sensitive Data necessary for any specific transaction or purpose. It is further the Company's policy that we do not collect certain biometric identifiers, which are fingerprints, retina or iris scans, scan of hand, voice prints, or scan of facial geometry. Sensitive Data includes any Personal Data, including but not limited to the following information:

- Customer name, address, email address, account numbers
- Financial account information, including credit or debit card numbers and bank account information and associated access codes, personal identification numbers (PINs)
- Social security numbers
- Taxpayer identification numbers
- Driver's license numbers or other state or national identification card numbers
- Usernames and passwords
- Digital identifiers, such as device IDs and cookie trackers

Non-Sensitive Data. Non-Sensitive Data is any Data that does not fall within the category of Sensitive Data. Non-Sensitive Data includes, without limitation:

- Public information: Information that has been or may be made available to the public, is not protected from disclosure, and that if disclosed will not jeopardize the privacy or security of the Company's employees, clients, partners and stakeholders. This includes information regularly made available to the public via electronic, verbal or hard copy media.
- Non-confidential information which (i) the unauthorized access, disclosure or destruction of that Data would not have an adverse impact on the Company if disclosed and (ii) has no legal or regulatory restrictions on its access or use.

Data Review and Destruction

All Data, whether stored electronically or on paper, should be reviewed on a regular basis (at least annually) to decide whether to destroy or delete any Data in accordance with this Policy. It is the Company's policy that we delete all Data once we no longer need the Data for a business purpose, provided that the Data is not contained within any Record listed under Appendix A, at which point the retention periods under Appendix A control. If Data is held on computer files, hard drives, memory sticks or other removable devices, this Data should be appropriately and irretrievable deleted or encrypted. Please note that simply deleting files from these devices using standard "delete" functions will not usually remove the file entirely. Please reach out to the IT department should you need support in permanently deleting such files.

Personal Data Access. Access to Personal Data should only be for:

(i) the purposes we collected the Personal Data for, such as accessing an email address to communicate an order status (unless we have a reason that is appropriate under applicable law to use such Personal Data for additional purposes – this exception should always be checked with the legal department),
(ii) responding to requests from a person who the Personal Data relates to,
(iii) for deletion in accordance with the retention periods in this Policy.

Access, use, and disclosure of Personal Data must at all times also comply with the Company's privacy notice, which is listed on the Company's website. If you are contemplating doing anything with Personal Data that is in contradiction to what is listed in the Company's privacy notice, you must contact legal and IT's security team before taking any further action with respect to such Personal Data.

Information Security. It is the Company's policy to take appropriate measures against the unauthorized access to or the unlawful processing of Data. It is also the Company's policy to take appropriate measures against the accidental loss, destruction or damage of Data. Such measures should be periodically tested and updated to remain in alignment with industry standards. For more information, please refer to IT's security protocols.

Data Handling. The handling, management, and maintenance of Data and the requirements of this Policy must be followed throughout the entire data lifecycle. The following requirements apply generally to Data, based on the category of the Data.

Non-sensitive data:

- Must be stored on the Company's secure file server or a Company-approved file storage system, such as Sharepoint, OneDrive, company databases, or company file shares.
- Modification of Non-Sensitive Data is restricted to authorized users who have a legitimate business need to modify the Data.

- Must be retained only for so long as there is a legitimate business need and as required by Appendix A.
- Must be disposed of in an appropriately secure manner. If you are unsure of how to appropriately dispose of Non-Sensitive Data, please contact IT.

Sensitive Data:

- Must be stored on the Company's secure file server or a Company-approved file storage system, such as Sharepoint, OneDrive, company databases, or company file shares.
- Requires file system encryption for Data at rest and requires encryption for Data in transit.
- Any customer account log-ins or portals must be secure and meet the Company's security standards.
- Sensitive Data may not be transmitted to a third party unless such transmission has been previously approved by legal and IT security.
- Transmission and storage of any regulated Sensitive Data must conform with applicable legal and regulatory requirements.
- Requires access controls, including physical, administrative, and technical safeguards, so that only those associates with a need to know are able and permitted to access the Sensitive Data.
- Modification of Sensitive Data may only be done by an associate authorized to modify such Data, who has a valid business need to modify the Data, and all Data modifications must be logged.
- Must be retained only for so long as there is a legitimate business need and in accordance with Appendix A.
- Must be disposed of in a secure manner. If you are unsure of how to securely dispose of Sensitive Data, please contact IT.

Suspension of Data and Record Disposal in the Event of Litigation or Claims.

In the event the Company is served with any subpoena or request for documents or any associate anticipates or becomes aware of a governmental investigation or audit concerning the Company or any actual or potential litigation against or concerning the Company, the associate shall inform the Legal Department. Upon the direction of the Legal Department, further destruction of Data and Records shall be suspended until such time as the Legal Department determines otherwise. This exception to the retention periods and the other requirements of this Policy is referred to as a litigation hold or a legal hold and is controlled by our Litigation Hold Policy. If you are ever placed under a litigation hold, the Litigation Hold Policy shall control and any retention periods or deletion or destruction recommendations under this Policy shall not apply during the litigation hold period. You will still be expected to store all Data and Records securely during the litigation hold. Once the litigation hold is lifted, this Policy shall once again control and govern all retention period and deletion or destruction recommendations.

Employee Termination or Retirement

Upon the termination or retirement of an associate, that associate's direct supervisor is responsible for examining (or causing to be examined) all Data, Records and other information held or maintained by the terminated or retired associate to ensure that this Policy is complied with and that Data and Records are transferred to the appropriate party or destroyed in accordance with this Policy. This review shall occur immediately upon the associate's departure from the Company. As the Company is the owner of all Records and Data, it is a violation of this Policy for an associate to clear, delete, or wipe their email, instant message, text message, call log, and other digital histories and paper files in advance of their departure from the Company. The associate's direct supervisor

shall coordinate with IT to ensure that access to Company systems that store Records and Data is restricted to current associates and other authorized parties.

Engaging Third Parties, Consultants, Contractors, or Subcontractors with Access to Data or Records

All third parties who are engaged to prepare, process, hold, archive, transmit, store, and/or delete Records or Data on the Company's behalf should be required to comply with specific data retention service levels, including (without limitation):

(a) to comply with the applicable provisions of this Policy;
(b) to only process the Records and Data we provide to them for purposes instructed to them by us;
(c) to keep the Company's Records and Data with sufficient security to prevent the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to such Records and Data.

These service levels should be agreed to in writing in a contract and executed in accordance with the Contracts Policy. Please contact the Legal Department in relation to engaging third party suppliers to prepare, process, hold, store, transmit, archive or delete Records and Data on the Company's behalf.

Retaliation Prohibited

The Company is committed to enforcing this Policy as it applies to all forms of Data, Records and Non-Records. The effectiveness of the Company'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 raise the matter with your department head, the CIO, or on Red Flag Reporting. If associates 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. No one will be subject to, and the Company prohibits, any form of discipline, reprisal, intimidation, or retaliation for reporting in good faith incidents of inappropriate conduct of any kind, pursuing any record destruction claim, or cooperating in related investigations.

Appendix A – RECORD RETENTION SCHEDULE

Records should be maintained for as long as indicated in this Schedule. Once the retention period for a Record has expired, the Record shall be destroyed unless a litigation hold has been issued by legal. The Record Retention Schedule is organized by section as follows:

A. Accounting and Finance Records
B. Corporate Books and Records
C. Correspondence and Internal Memoranda
D. Customer Data and Databases
E. Electronic Records
F. Employment and Benefits Records
G. Legal Records
H. Operations Records
I. Regulatory Records
J. Risk Management Records
K. Tax Records

A. ACCOUNTING AND FINANCE RECORDS

Record Type	Retention Period
Accounts Payable ledgers and schedules	7 years
Accounts Receivable ledgers and schedules	7 years
Annual Audit Reports and Financial Statements	Permanent
Annual Audit Records, including work papers and other documents that relate to the audit	7 years after completion of audit
Annual Plans and Budgets	2 years
Bank Statements and Canceled Checks	7 years
Contributions and gifts Records	Permanent
Debt agreements, compliance certificates and related Records	10 years
Depreciation Schedules	Permanent
Expense Reports	7 years

General Ledgers	Permanent
Interim Financial Statements	7 years
Notes Receivable ledgers and schedules	7 years
Investment Records	7 years after sale of investment
Internal Audit work papers and findings	7 years after completion

B. CORPORATE BOOKS AND RECORDS

Record Type	Retention Period
Corporate Books, including organizational documents, agreements, shareholder Records, certificates, minutes of meetings, qualifications and related Records	Permanent
Board and committee membership, meeting materials and related Records	Permanent
Business Licenses and Permits	Permanent

C. CORRESPONDENCE & INTERNAL MEMORANDA

If correspondence and internal memos contain material information related to the document or transaction they support, then those memos and correspondence should be retained for the same period of time as the document they relate to or support. For example, a letter containing material information related to a particular contract should be retained as long as the required contract retention period, whereas an email stating only "Thanks for the call to discuss our contract!" can be deleted promptly.

Correspondence or memos that do not pertain to documents having a prescribed retention period fall into two separate categories. The two general categories are as follows:

1. Correspondence or memos related to routine matters and having no significant, lasting consequences should be discarded promptly, or at the latest within twelve months. Some examples include:
    - Routine letters and notes that require no acknowledgment or follow-up, such as notes of appreciation, congratulations, letters of transmittal, and plans for meetings.
    - Form letters that require no follow-up.
    - Letters of general inquiry and replies that complete a cycle of correspondence.
    - Other letters of inconsequential subject matter or that close correspondence to which no further reference will be necessary.

2. Correspondence and memos related to non-routine matters and having significant lasting consequences should generally be retained permanently.

D. CUSTOMER RECORDS & DATA

Record Type	Retention Period
Customer Account Records	7 years following the date of closure of the customer's account
Customer Data	In general, unless customer Data falls under Records in a separate category within this Schedule A, a legal hold, or is subject to separate legal or regulatory requirements, customer Data should only be maintained and stored for as long as the customer Data is needed and serves a business purpose.
Customer requests regarding their Personal Data, including requests to know what information we collect on them, that their information be deleted, or that we do not sell their information.	2 years after date of the customer request, or for any longer period identified by the legal department.
Logs of modifications made to customer's Personal Data	Maintain for two years after that customer's account was last active.

E. ELECTRONIC DOCUMENTS

1. **Electronic Documents used for Communication and Tasks (i.e. Email, Instant Messages, Text Messages, etc.):** Not all documents used for communication and task management need to be retained, depending on the subject matter. In fact, all such documents that are not Records addressed elsewhere in this Schedule should be securely destroyed at the time they are no longer needed and routinely or automatically after a set period of time.

    - Associates must not store or transfer Company related email on or to non-work-related computers.
    - Associates must take care not to send confidential or proprietary information to unauthorized recipients (including any Personal Data).
    - All electronic documents other than Records used for communication and task management must be deleted after a maximum period of 1 year unless there is a business justification to keep them.
    - Some electronic document and communication systems have automatic deletion schedules associated with them. These automatic deletion schedules are listed below:
        - Email: Automatically deleted after 12 months.
        - Instant Messages, such as Slack: Automatically deleted after 90 days.

If you have an electronic document or communication which is a Record as described in this Schedule and therefore must be retained or preserved for a period longer than the above automatic deletion schedule, then it is your responsibility to store that document or communication elsewhere prior to the Record being automatically deleted. The preferred storage method is within your work-issued OneDrive or SharePoint files. Associates are prohibited from storing any work documents or communications in personal files or drives, such as an Associate's personal Google Drive account. Legal holds will automatically prevent email communications from being deleted on an automatic schedule until the legal hold is released.

The following departments shall also be subject to the automatic deletion of emails, but instead of emails being deleted after 12 months, emails will not be deleted until after the time period noted below for each corresponding department:

HR: 3 Years **Tax:** 7 Years **Legal:** 3 Years **Audit:** 7 Years **Finance (including Accounting & Payroll):** 3 Years

2. **Other Electronic Documents:** Other examples of electronic documents include the following: forms, reports, manuals, notes, calendars, diaries, drafts, copies, spreadsheets, word-processing documents, multi-media files and presentations, voice mail and other digital media, such as video recordings, audiotape, photographs. These types of digital files are also subject to this Policy and their retention period depends on whether or not they are Records, as well as the applicable subject matter.

F. EMPLOYMENT AND BENEFITS RECORDS

Record Type	Retention Period
Associate benefit plans subject to ERISA (includes plans regarding health and dental insurance, 401K, long-term disability, and Form 5500)	6 years
Benefits descriptions	Permanent
Associate applications and resumes	4 years
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
Collective Bargaining Agreements and related Records	3 years
Employment and Separation Agreements	3 years from their last effective date
I-9 Forms	3 years after date of hire or 1 year after employment is terminated, whichever is later
Incentive plans, commissions and related Records	7 years
Payroll registers (gross and net)	Permanent

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
Policies and Procedures	Permanent
Training, certifications and qualification Records	10 years

G. LEGAL RECORDS

Record Type	Retention Period
Acquisition Records including non-Disclosure agreements, indications of interest and letters of intent, information memorandums, process letters, diligence materials, post-closing correspondence and related Records	Permanent
Court Orders	Permanent
Closing Sets	Permanent
Contracts and agreements and related correspondence (including any proposal that resulted in the contract, as well as all change orders and all other supportive documentation)	7 years after expiration or termination of the account; permanent for insurance contracts
Deeds of title and other real estate documents (including loan and mortgage contracts)	Permanent
Government contracting compliance Records	10 years
Independent contractor agreements and related documentation	7 years after expiration
Intellectual property portfolio Records, including copyright, trademark and domain name registrations, licenses	Permanent
Investigation files	Permanent for open investigations, 10 years for closed
Leases, amendments and related Records	Permanent for active leases, 6 years for expired
Legal Memoranda and Opinions (including all subject matter files)	10 years after close of matter

Litigation and Claims files	10 years after expiration of appeals or time for filing appeals
Policy Records, including policies, violations of policies and requests for departures from policies	Permanent
Vehicle registrations and maintenance logs	Permanent for active vehicles, 2 years for disposed of vehicles

H. OPERATIONS RECORDS

Record Type	Retention Period
Credit Applications (customer and vendor)	Life of the customer/vendor account. If the application was denied or if the account had a shorter lifespan, then retain at least 25 months for consumers and 12 months for businesses.
Customer complaints, repair and replace demands and remediation Records	2 years after resolution
Delivery Records	1 year
Design services Records, including CAD drawings and related Records	6 years from the last use or modification of the drawing/file
Lien and collections Records	10 years from date of payoff
Purchase orders and related correspondence	7 years or longer if a warranty period is longer than 7 years
Policy and Procedures Manuals – Original	Current version with revision history
Policy and Procedures Manuals - Copies	Retain current version only
Project files	7 years following project completion
Product Warranties	Retain for 7 years after warranty expired
Receipts (Cash and Credit)	3 years

I. MISCELLANEOUS

Record Type	Retention Period
Consultant's Reports	2 years
Material of Historical Value (including pictures, publications)	Permanent
Annual Reports	Permanent

J. REGULATORY RECORDS

Record Type	Retention Period
Citations, tickets and other administrative penalties	As directed by the Legal Department
Environmental studies	Permanent
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
Hazardous material exposures	Duration of employment + 30 years
Department of Transportation DVIR Records	At least 1 year from the date the report was prepared
Import/ export Records	5 years or the minimum required by applicable law, whichever is greater
Regulatory interactions including audits, requests for information and investigations	As directed by the Legal Department
Records evidencing compliance with regulatory requirements	Permanent

K. RISK MANAGEMENT RECORDS

Record Type	Retention Period
Insurance Policies	Permanent

Claims files and related Records	Permanent

L. TAX RECORDS

The Company must keep books of account or records in order to establish the amount of gross income, deductions, credits, or other matters required to be shown in any such return. These documents and records shall be kept for as long as they may become material in the administration of federal, state, and local tax laws.

Record Type	Retention Period
Tax-Exemption Documents and Related Correspondence	Permanent
IRS Rulings	Permanent
Excise Tax Records	7 years
Tax Bills, Receipts, Statements	7 years
Tax Returns - Income, Franchise, Property	Permanent
Tax Work paper Packages - Originals	7 years
Sales/Use Tax Records	7 years
Annual Information Returns - Federal and State	Permanent
IRS or other Government Audit Records	Permanent