Data Retention & Deletion Policy

Document creation Date:	June 15, 2025
Effective Date:	July 2, 2025
Version:	1.2
Classification:	Public

1. Purpose

This Data Retention Policy establishes the procedures used by Divy It Up, LLC (the "Company") to manage the full lifecycle of data collected, processed, stored, or transmitted by its systems.

The purpose is to ensure that data is retained only as long as necessary for legitimate operational, legal, regulatory, or security purposes, and that data is securely deleted or anonymized when no longer required. This policy supports the Company's commitments to data minimization, privacy, and regulatory compliance while maintaining service functionality and security.

2. Scope

This policy applies to:

- All Company systems and infrastructure
- All data stored in Company databases, logs, backups, and storage systems
- All customer information collected through web and mobile applications
- All third-party integrations (including Plaid and financial service providers)
- All employees, contractors, and service providers who handle Company data

3. Data Minimization Principle

The Company adheres to strict data minimization: it collects and retains only the information necessary to deliver its services, fulfill legal obligations, and protect security.

Unnecessary personal or financial information is never collected. Where possible, data is pseudonymized or anonymized to reduce risk.

4. Data Classification Reference

All data is classified according to the Company's Information Security Policy. Retention requirements are applied based on the following categories:

- Public Data
- Internal Data
- Sensitive Data (financial account information, PII, authentication tokens, API credentials, transaction metadata)

Sensitive data receives the highest level of protection and shortest feasible retention periods.

5. Retention Schedule

Data is retained only for as long as required for operational, legal, security, or compliance purposes. The following table defines standard retention periods:

Data Type	Retention Period	Justification / Trigger for Deletion	Deletion Method
User account records	While account is active + 30 days	Account closure or user deletion request	Secure database deletion
Financial integration tokens	While integration is active + 7 days	Integration revoked or token expiration	Immediate token revocation
Transaction metadata	Duration of active service + 1 year	End of service or legal hold expiration	Automated deletion scripts
System & security logs	90 days (operational) / 1 year (security)	Log rotation schedule	Secure overwrite
Error & monitoring data	90 days	Operational troubleshooting completed	Automated purge
Backup data	30 days (daily) / 90 days (weekly/monthly)	Backup lifecycle policy	Encrypted & auto-expired
Audit & compliance records	7 years (or as required by law)	Regulatory or contractual obligation	Secure archive then deletion

Exceptions require written approval from the Security Officer and Legal/Compliance.

6. Secure Deletion Procedures

When data reaches the end of its retention period, the Company applies secure deletion methods aligned with NIST SP 800-88 guidelines:

- Database record deletion with cascading removal
- Secure file deletion (overwrite with random data)
- Cryptographic erasure of encrypted volumes
- Immediate revocation and purging of API tokens and credentials
- Automated lifecycle policies in cloud storage and databases

Where full deletion is not feasible (e.g., for analytics), data is irreversibly anonymized.

7. Deletion Verification

After deletion, the Company verifies:

- Data is no longer accessible in active systems
- Backups have been purged or expired
- Third-party integrations have been notified (if applicable)
- A deletion log entry is recorded for audit purposes

8. User-Requested Data Deletion (Right to be Forgotten)

Users may submit a verified request to delete their account and associated data. Upon receipt, the Company will:

1. Verify the requester's identity
2. Deactivate the account immediately
3. Revoke and delete all associated integration tokens
4. Delete or irreversibly anonymize user records within 30 days
5. Confirm completion to the user

Certain data may be retained longer if required for fraud prevention, legal holds, or regulatory compliance. The user will be informed of any such exceptions.

9. Backup and Archive Data

Backup copies are retained only for disaster recovery purposes and are not used for active processing. Backups are:

- Encrypted at rest
- Access-restricted to authorized personnel
- Automatically rotated and expired per the backup policy
- Excluded from operational data stores

10. Third-Party Data Handling

When data is shared with trusted third-party providers (e.g., cloud infrastructure, Plaid), the Company:

- Shares only the minimum data necessary
- Requires contractual data-protection and retention clauses
- Regularly reviews third-party compliance

Third parties are responsible for their own retention practices within the bounds of our agreements.

11. Responsibilities

- Security Team: Oversees policy implementation, deletion automation, and audits
- Engineering/DevOps: Implements technical retention controls and deletion scripts
- Legal/Compliance: Reviews retention periods for regulatory alignment
- All Personnel: Report any suspected improper data retention or deletion issues

12. Auditing and Compliance

The Company conducts annual audits of data retention practices. Audit logs include:

- Deletion events and verification
- Exceptions granted
- User deletion requests and outcomes

Results are documented and retained for compliance review.

13. Policy Review and Updates

This policy is reviewed at least annually or after any significant operational, legal, or regulatory change. Updates are approved through the same governance process as the Information Security Policy.

14. Contact Information

Questions or concerns regarding data retention or deletion should be directed to:

Security & Compliance Team Divy It Up, LLC security@divyitup.com

Revision History

Version	Date	Description	Author
1.0	July 2, 2025	Initial formal release	Security & Legal Team