



AIZYNE

Aizyne Vault

Complete User Guide

For new and experienced users managing encrypted records, documents, recovery and backups on Windows.

Release scope. Version 1.0 supports x64 Windows 11. The application is free with no trial, subscription, in-app purchase or paid feature.

Version 1.0 | 10 October 2026

Support: info@aizynegroup.com

Privacy: <https://aizynegroup.com/vault-privacy>

About. About this guide

This guide explains initial setup, daily use, privacy boundaries, recovery and backup verification for Aizyne Vault.

Read this first. Aizyne Group cannot reset a forgotten master passphrase or recover a vault unless you prepared a valid recovery route. Complete the setup checklist and check a backup before depending on the vault.

Who this guide is for

- New users creating their first encrypted vault.
- Experienced users managing records, attachments and reminders.
- People preparing recovery, transfer or backup arrangements.
- Anyone reviewing privacy and security behaviour before use.

Contents

- 1 Quick start
- 2 What Aizyne Vault does
- 3 Installation and first launch
- 4 Create the vault
- 5 Setup checklist
- 6 Workspace and navigation
- 7 Records and organisation
- 8 Sensitive values and clipboard
- 9 Documents and attachments
- 10 Versions reminders and history
- 11 Security locking and Windows Hello
- 12 Recovery
- 13 Backups and restore
- 14 Portable copies export and import
- 15 Emergency access
- 16 Archive recycle bin and deletion
- 17 Password tools
- 18 Accessibility
- 19 Privacy and data boundaries
- 20 Updates migration and uninstall
- 21 Troubleshooting
- 22 Frequently asked questions
- 23 Glossary
- 24 Support

1. Quick start

Complete the safety steps before storing important information.

Step	Action	Reason
1	Install from Microsoft Store.	Use the official signed release and required runtime.
2	Create a vault with a unique master passphrase.	The passphrase controls access and cannot be reset by Aizyne.
3	Lock and unlock once.	Proves you can regain access.
4	Prepare and confirm recovery material.	Provides a planned recovery route.
5	Create and check an encrypted backup.	Proves a separate copy authenticates and reopens.
6	Optionally configure Windows Hello.	Adds convenient device-bound access.
7	Create records and attachments.	Begin ordinary use after setup is complete.

Keep access routes separate. Do not keep the only backup, master passphrase and recovery material together on the same device.

2. What Aizyne Vault does

Aizyne Vault stores structured records and document attachments in a local encrypted vault.

Capability	Purpose
Five record types	Logins, secure notes, recovery information, identity records and documents.
Organisation	Collections, tags, favourites, search, archive and recycle bin.
Attachments	Encrypted file copies held inside Document records.
Recovery	Prepared recovery material and optional Windows Hello.
Backups	Create, check and restore encrypted copies without replacing the live vault during verification.
Exports	Readable copies created only through an action you choose.
Reminders	Generic Windows notifications without titles or private details.

Security boundary. Encryption protects the stored vault while locked. It cannot protect an unlocked device from malware, screen capture, an administrator or another person controlling Windows.

3. Installation and first launch

Install the released application from its official Microsoft Store listing.

1. Open the Aizyne Vault Microsoft Store listing.
2. Select Get or Install.
3. Let Windows finish installation and runtime setup.
4. Open Aizyne Vault from Start or the Store page.

First launch

Read the access and recovery warning. The app creates one local encrypted vault and does not require an Aizyne account.

Use the official listing. Do not install packages sent by email or obtained from an unknown website.

4. Create the vault

The master passphrase is the primary route into the vault.

1. Choose Create vault.
2. Enter a unique, long passphrase not used elsewhere.
3. Confirm the same passphrase.
4. Read the recovery warning and create the vault.

Passphrase guidance

Choose a phrase you can enter accurately. Do not keep the only copy in the vault it unlocks. Aizyne Group does not receive the passphrase and cannot reset it.

Permanent loss is possible. Losing every valid access and recovery route can make the vault permanently unreadable.

5. Setup checklist

The checklist links the tasks that should pass before ordinary record entry.

Check	Completed when
Create the encrypted vault	The new vault saves successfully.
Check passphrase access	You lock and unlock with the passphrase.
Prepare and confirm recovery	Recovery material is created and verified.
Create and check the first backup	A separate encrypted backup authenticates and reopens.

A completion time records what passed at that moment. It does not guarantee that recovery material or a backup still exists later. Recheck after significant changes.

6. Workspace and navigation

The unlocked workspace groups related work into task-focused areas.

Area	Use
Records	Create, search, organise and manage records and attachments.
Security and recovery	Locking, access, recovery material and Windows Hello.
Backup and transfer	Create, check, restore and save encrypted copies.
Export selected	Create deliberate readable exports.
Import records	Review and import supported record data.
Emergency access	Prepare controlled emergency information.
Reminders	Review and manage reminders.
Setup checklist	Confirm access, recovery and backup readiness.

Use the task guide for linked workflows such as Add document with attachment, Back up my vault or Prepare recovery. It moves directly to the next required step.

7. Records and organisation

Choose the record type that best matches the information.

Type	Typical contents
Login	Username, password, website and access notes.
Secure note	Private text or structured information.
Recovery information	Recovery codes, instructions and access details.
Identity record	Identity details and supporting references.
Document	Description, reference and encrypted attachments.

Create a record

1. Choose Add record or a task-guide shortcut.
2. Select the type.
3. Enter title, subtitle, collection and useful tags.
4. Complete the type-specific fields.
5. Choose Create and encrypt.

Find and manage records

- Search titles, subtitles, collections, tags and ordinary fields.
- Filter by collection, tag, favourite status or location.
- Clear filters if a record seems missing.
- Edit a selected record; the previous version remains concealed for review.

8. Sensitive values and clipboard

Passwords and recovery values remain concealed until deliberately revealed or copied.

1. Choose Reveal sensitive fields to show them briefly.
2. Choose Copy beside only the required field.
3. Paste into the intended destination.
4. Confirm the clipboard has cleared or been replaced before continuing.

Aizyne Vault asks Windows to exclude the copy from clipboard history and device synchronisation. It attempts to clear its copy after the selected interval while the clipboard still holds that same value.

Clipboard limits. Other applications can read clipboard content before clearing. Clearing cannot recall a value already pasted or captured elsewhere.

9. Documents and attachments

A Document record holds descriptive fields and one or more encrypted file copies.

Add a document with its attachment

1. Choose Add document with attachment from the task guide.
2. Enter the title and optional description or reference.
3. Create and encrypt the Document record.
4. Choose Add encrypted attachment and select the file.
5. Enter the master passphrase when requested.
6. Confirm the name and size appear in the record.

Export an attachment

1. Select the attachment.
2. Enter the master passphrase and acknowledge that a readable file will remain outside the vault.
3. Choose Export selected attachment and a destination.
4. Check the success message and remove the readable file when finished.

Outside copies remain. The original file is unchanged. An exported attachment is another readable copy and must be removed separately.

10. Versions reminders and activity history

Previous versions

Edits create concealed previous versions. Select a record and choose Go to previous versions while the vault is unlocked.

Activity history

Activity history uses allowlisted action categories and neutral descriptions. Sensitive values and unrecognised summaries are never shown.

Reminders

1. Select a record and choose Go to reminder.
2. Set the date, time and recurrence where available.
3. Save and review it from Reminders.
4. Open and unlock the vault to see the associated private record.

Windows receives the scheduled time and an opaque identifier. Notification wording is generic; Windows controls delivery and notification history.

11. Security locking and Windows Hello

Event	Expected result
Lock now	Vault closes immediately and passphrase controls clear.
Close window	Vault locks.
Windows locks or suspends	Vault locks.
Inactivity threshold	Vault locks after the chosen interval.

- Use Ctrl + Shift + L to lock quickly.
- Keep Windows current and use a separate account for each person.
- Do not leave readable exports open after use.

Windows Hello

Windows Hello is an optional device-bound convenience route. Configure it only after the master passphrase and recovery route are established. Keep both even after Hello works.

12. Recovery

Recovery succeeds only when valid material was prepared, confirmed and retained.

1. Open Security and recovery.
2. Create recovery material and save it in the intended secure location.
3. Read the warning about outside copies.
4. Confirm recovery through the verification flow.
5. Record where the material is kept without copying the secret into an insecure note.

Test safely. Use the supported verification or separate-copy workflow. Do not overwrite the only live vault while proving recovery.

13. Backups and restore

A backup is trustworthy only after it has authenticated and reopened.

Create and check

1. Open Backup and transfer.
2. Enter the passphrase and acknowledge where the copy remains.
3. Create the encrypted backup.
4. Choose Check encrypted backup.
5. Confirm a separate copy reopened and the current vault was unchanged.

Restore as a separate copy

1. Select a known backup.
2. Enter the required passphrase.
3. Restore as a separate encrypted copy.
4. Confirm the restored copy authenticates and matches the backup.
5. Remove the restored verification copy after review.

Use more than one location. Keep at least one checked backup away from the device containing the live vault.

14. Portable copies export and import

Portable encrypted copy

Create a portable copy for deliberate transfer or separate custody. Keep its opening information separately and verify it on the destination through the supported workflow.

Readable record export

1. Select only the required records.
2. Review the included fields and destination.
3. Enter the passphrase and acknowledge that the output is readable.
4. Complete the export, review every field and remove it when no longer needed.

Import records

1. Choose a supported import file.
2. Review counts, mappings and warnings.
3. Exclude unwanted items.
4. Confirm the import and inspect the resulting records before deleting the source.

Review before sharing. Exports can contain more context than expected. Check the complete readable copy before sending it.

15. Emergency access

Prepare the minimum information another person would need for the chosen emergency scenario.

- Name the purpose and intended recipient.
- Select only the required records or instructions.
- Review recovery dependencies and readable wording.
- Create the controlled package or summary.
- Test the intended opening route.
- Record where each required part is kept.

Review emergency arrangements after changes to people, devices, passphrases, recovery material or storage locations.

16. Archive recycle bin and deletion

Action	Result
Archive	Retains a record outside the normal active list.
Restore from archive	Returns it to Active.
Move to Recycle Bin	Removes it from Active but allows restoration.
Restore from Recycle Bin	Returns it to Active.
Delete permanently	Removes it from the current vault after confirmation.

Other copies may remain. Older backups, previous generations, exports and other applications may retain deleted information. Remove those copies separately.

17. Password tools

Password and passphrase generation and review operate locally.

- Generate a 20-character password for services that accept complex passwords.
- Generate an eight-word passphrase when length and memorability are suitable.
- Use local password review to identify weak or reused active Password fields without displaying or transmitting values.

Change the service first. Editing a vault field does not change the credential on a website or service. Verify the service change, then update the vault.

18. Accessibility

Aizyne Vault supports keyboard navigation, visible focus, high contrast and screen-reader descriptions.

Shortcut	Action
Ctrl + F	Move to record search.
Ctrl + Shift + R	Open Records.
Ctrl + Shift + L	Lock the vault.

- Use Tab and Shift + Tab to move through controls.
- Use Enter or Space to activate the focused control.
- Use Windows high contrast and text scaling as needed.
- Let Narrator finish the current control before changing screens.

19. Privacy and data boundaries

Information or service	Behaviour
Vault records and attachments	Stored locally in the encrypted vault.
Aizyne accounts analytics or advertising	No such service receives vault content.
Windows Hello	Windows provides device-bound authentication.
Notifications	Windows receives time and an opaque identifier; wording is generic.
Backups exports portable copies	Saved only through actions you choose and remain until removed.
Support summary	Prepared locally and copied only when you choose.

Read the current policy at <https://aizynegroup.com/vault-privacy>. Encryption protects stored information while locked but cannot prevent access by malware, an administrator, screen capture or another person controlling an unlocked device.

20. Updates migration and uninstall

Before an update

- Create and check a fresh encrypted backup.
- Keep recovery material available.
- Close Aizyne Vault normally.

After an update

- Open and unlock the vault.
- Confirm records, attachments and setup status.
- Check a representative backup and export or attachment workflow when storage behaviour changed.

Before uninstalling

- Create and check a backup if the vault must be retained.
- Record where external backups, exports and portable copies are stored.
- Understand that uninstalling may not remove files deliberately saved outside app-private storage.

21. Troubleshooting

Preserve the live vault and every backup while investigating.

Problem	What to try
Cannot unlock	Check keyboard layout, Caps Lock and Num Lock; try Windows Hello or prepared recovery.
Record missing	Clear filters and check Archived and Recycle Bin.
Reminder missing	Check Windows notification and Focus settings.
Attachment export failed	Choose a writable folder, check space and re-enter the passphrase.
Backup check failed	Keep copies unchanged; verify the passphrase and try another known backup.
Windows Hello unavailable	Use the master passphrase, then review Hello configuration.
App closes or locks	Reopen, unlock and record exact non-sensitive error wording.

Do not send secrets. Support never needs a passphrase, recovery key, vault, backup, readable export or private screenshot.

22. Frequently asked questions

Does Vault need an online account?

No. Vault content is local and no Aizyne account is required.

Can Aizyne reset my passphrase?

No. Use a valid prepared recovery or Windows Hello route.

Are attachments encrypted?

The copy inside the vault is encrypted. Originals and exports remain separate readable files.

Does checking a backup replace the live vault?

No. Check and restore-as-separate-copy workflows preserve the current vault.

Are reminders private?

Wording is generic, but Windows controls scheduling and notification history.

Is the program free?

Yes. There is no charge, trial, subscription, in-app purchase or paid feature.

Does Release 1 support ARM64?

No. Release 1 is x64 Windows 11; ARM64 is deferred.

Has it received independent security approval?

No. Release preparation records internal review only.

23. Glossary

Term	Meaning
Active record	A record in the normal working list.
Archive	A retained record removed from Active.
Attachment	A file copy encrypted inside a Document record.
Encrypted backup	A separate encrypted copy of the vault.
Master passphrase	The primary secret used to unlock the vault.
Portable copy	An encrypted package for transfer or separate custody.
Readable export	Information copied outside the vault without vault encryption.
Recovery material	Prepared information used by the supported recovery flow.
Recycle Bin	A holding area before permanent deletion.
Windows Hello	Optional device-bound Windows authentication.

24. Support

Current guidance is available at <https://aizynergroupp.com/vault-support>

When asking for help

- Describe the operation you attempted.
- Include the Aizyne Vault and Windows versions.
- Confirm whether the device is x64.
- Copy the exact non-sensitive error wording.
- State whether the problem repeats.

Protect your information. Remove usernames, paths, record titles and private details. Never attach a vault, backup, export, recovery material or secret-bearing screenshot.

Email: info@aizynergroupp.com

Privacy policy: <https://aizynergroupp.com/vault-privacy>