

PathwAI

Confidentiality Policy

Version 1 - Approved by Abdullah Adeeb

Confidentiality Policy

Policy brief & purpose

PathwAI Labs is committed to safeguarding the confidentiality of the data in its possession. Our customers and other stakeholders depend on us to protect the confidentiality of the data collected by us or shared with us.

We have designed this policy to explain how we expect our staff to treat confidential information. Employees will unavoidably receive and handle confidential information about customers, partners, and our company. We want to make sure that this information is well-protected.

We must protect this information for two reasons. It may:

1. Be legally binding (e.g. GDPR, HIPAA, customer contracts, etc).
2. Constitute the backbone of our business, giving us a competitive advantage (e.g. business processes.).

Scope

This policy affects all staff (whether employees or contractors), board members, contractors, and volunteers, who may have access to confidential information.

Policy elements

Confidential and proprietary information is secret, valuable, expensive, and/or easily replicated. Common examples of confidential information are:

1. Unpublished financial information.
2. Data of customers/partners/vendors.
3. Patents, formulas, or new technologies.
4. Customer lists (existing and prospective).
5. Data entrusted to our company by external parties.
6. Pricing/marketing and other undisclosed strategies.
7. Documents and processes explicitly marked as confidential.
8. Unpublished goals, forecasts, and initiatives marked as confidential.

Employees may have various levels of authorized access to confidential information.

What we should do:

1. Lock or secure confidential information at all times.
2. Shred physical confidential documents when they're no longer needed.
3. Make sure we view confidential information only on secure devices.
4. Only disclose information to other staff when it's necessary and authorized.

5. Keep confidential documents inside the company premises unless it's absolutely necessary to move them.
6. When employees stop working for our company, they're obliged to return any confidential files and delete them from their personal devices.

What we shouldn't do:

1. Use confidential information for any personal benefit or profit.
2. Disclose confidential information to anyone outside of our company.
3. Replicate confidential documents and files and store them on insecure devices.

Confidentiality Measures

We'll take measures to ensure that confidential information is well protected. We'll:

1. Store and lock paper documents.
2. Encrypt electronic information and safeguard databases.
3. Ask employees to sign non-compete and/or non-disclosure agreements (NDAs).
4. Ask for authorization by senior management when it is necessary to allow employees to access certain confidential information.

Exceptions

Confidential information may occasionally have to be disclosed for legitimate reasons. Examples are:

1. If a regulatory body requests it as part of an investigation or audit.
2. If our company examines a venture or partnership that requires disclosing some information (within legal boundaries).
3. In such cases, employees involved should document their disclosure procedure and collect all needed authorizations. We're bound to avoid disclosing more information than needed.

Non-compliance

Employees who don't respect our confidentiality policy will face disciplinary and, possibly, legal action. We'll investigate every breach of this policy. We'll terminate any staff who wilfully or regularly breaches our confidentiality guidelines for personal profit. We may also have to punish any unintentional breach of this policy depending on its frequency and seriousness. We'll terminate employees who repeatedly disregard this policy, even when they do so unintentionally. This policy is binding even after the separation of employment.

Questions

If you have any questions regarding this policy, please reach out to the policy owner.

End of Confidentiality Policy. For version history, please see the next page.

Version History

Version	Log	Date
1	Current Policy version approved by Abdullah Adeeb	02 Dec, 2025
1	New policy version created	02 Dec, 2025