

## Member Confidentiality Policy

**Written By:** Peter Verhagen  
**Approved By:** Luke Martin  
**Endorsed By:** Kristyn Adamopoulos  
**Review Date:** 10/6/21

---

We designed our company Confidentiality Policy to explain how we expect our members to treat confidential information. Managers/department heads/committee members will unavoidably receive and handle personal and private information about members, patrons and our company. We want to make sure that this information is well-protected.

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

- Be legally binding (e.g. sensitive customer data.)
- Constitute the backbone of our business, giving us a competitive advantage (e.g. business processes.)

### Scope

This policy affects all members, including committee members, investors, 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:

- Unpublished financial information
- Data of Members/Patrons/The Company
- Patents, formulas or new technologies
- Customer lists (existing and prospective)
- Data entrusted to our company by external parties
- Pricing/marketing and other undisclosed strategies
- Documents and processes explicitly marked as confidential
- Unpublished goals, forecasts and initiatives marked as confidential
- Inter-committee communications, such as meeting minutes, email exchanges or slack messages.

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

#### What members should do:

- Lock or secure confidential information at all times
- Shred confidential documents when they're no longer needed
- Make sure they only view confidential information on secure devices
- Only disclose information to other members when it's necessary and authorized
- Keep confidential documents on the company Shared Drive.

#### What members should not do:

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

*This document was developed utilising and adapting content from:*

<https://resources.workable.com/confidentiality-company-policy>

When a member finishes their respective production or their membership lapses, they're obliged to return any confidential files and delete them from their personal devices.

### Confidentiality Measures

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

- Store and lock paper documents
- Encrypt electronic information and safeguard databases
- Ask for authorization by senior management to allow members to access certain confidential information

### Exemptions

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

- If a regulatory body requests it as part of an investigation or audit
- If our company examines a venture or partnership that requires disclosing some information (within legal boundaries)

In such cases, members involved should document their disclosure procedure and collect all needed authorizations. We're bound to avoid disclosing more information than needed.

### Disciplinary Consequences

Members 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 member 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 members who repeatedly disregard this policy, even when they do so unintentionally.

This policy is binding even after separation of employment, or a financial membership lapses.