Anthropocene Alliance
info@anthropocenealliance.org

anthropocenealliance.org

Accountability

The following document includes the following policies:

- Terms of Use
- Privacy
- Donor Privacy
- Whistleblower
- IT and Data
- Conflict of Interest

If you have questions about these policies, please contact us at: Anthropocene Alliance
Attn: Michelle Smith, 382 NE 191st St., PMB 983872, Miami, FL 33179
Info@anthropocenealliance.org

Date of Last Revision: December 23, 2024

Terms of Use (website)

Overview: Anthropocene Alliance (A2) operates and hosts the online environments accessible through https://anthropocenealliance.org. By accessing or using this website, you agree to comply with these Terms of Use. If you do not agree, please do not use the website.
Your compliance with these Terms of Use is a condition of your continued access. Breaching any provision of these Terms will result in the automatic termination of your right to access the website without prior notice. Violations may subject you to legal claims including, but not limited to, conversion, misappropriation, and trespass to chattels.

Links to Third-Party Websites: We may provide links to third-party websites for convenience. A2 does not review, control, or endorse these websites and is not responsible for their content, products, services, or practices. Accessing these websites is at your own risk and subject to the terms and conditions of the respective sites. If you have questions regarding a linked site, please contact its webmaster.

Intellectual Property Rights: All content on this website, including but not limited to text, images, logos, and software, is protected under copyright, trademark, trade secret, and other applicable intellectual property laws. Unless expressly stated otherwise, you are granted no

rights to use, reproduce, modify, or distribute the content. Unauthorized use of any materials may result in legal action.

User Conduct: By using this website, you agree to:

- Use the website in a lawful manner and for its intended purposes.
- Refrain from engaging in any activities that could harm, disrupt, or interfere with the website's operations.
- Not attempt to gain unauthorized access to the website or its associated systems.

Disclaimer of Warranties: The website and its content are provided "as is" and "as available" without warranties of any kind, either express or implied. A2 disclaims all warranties, including but not limited to implied warranties of merchantability, fitness for a particular purpose, and non-infringement. We do not guarantee that the website will be error-free, secure, or continuously available.

Limitation of Liability: To the fullest extent permitted by law, A2 shall not be liable for damages arising out of or related to use of the website. This includes, but is not limited to, direct, indirect, incidental, consequential, and punitive damages, even if we have been advised of the possibility of such damages.

Changes to the Terms of Use: We may update these Terms of Use from time to time. Significant changes will be communicated through our website or other appropriate means. By continuing to use the website after changes are posted, you agree to the updated terms.

Governing Law: These Terms of Use are governed by and construed in accordance with the laws of Florida. Any disputes arising under these Terms shall be resolved exclusively in the courts of Florida.

Privacy

Overview: A2 collects certain non-personally-identifying and personally-identifiable information to improve our services and enhance your browsing experience. This Privacy Policy outlines how we collect, use, and protect your data, as well as your rights concerning your personal information.

Non-Personally-Identifying Information: We collect non-personally-identifying information such as browser type, language preference, referring site, and the date and time of each visitor request. This data helps us understand how visitors use our website and improve its functionality. From time to time, we may release aggregated, non-personally-identifying information to the public, such as usage trends.

Personally-Identifying Information: By using our website, you consent to the collection, processing, storage, and disclosure of your personally-identifiable information as outlined below.

We collect personally-identifying information only when you voluntarily provide it, such as by registering, filling out forms, or engaging in other website activities. The type of information collected depends on the interaction and may include:

- Name
- Email address
- Contact information
- Other details you choose to provide

You can refuse to supply personally-identifying information; however, this may limit your ability to use certain website features.

Use of Collected Information: We use personally-identifying information solely to fulfill the purposes for which it was provided, such as:
- Responding to your inquiries
- Providing requested services
- Improving the website's content and functionality

Cookies: Cookies are small data files stored on your device to enhance your browsing experience. We use cookies for purposes such as:
- Managing session activities (e.g., maintaining login status)
- Analyzing website usage for performance improvement
- Recognizing returning visitors

You can manage or disable cookies through your browser settings. Note that disabling cookies may affect website functionality. For more details, visit All About Cookies.

Data Protection and Security: We implement reasonable security measures to protect your information from unauthorized access, alteration, or destruction. These measures include encryption, secure servers, and periodic reviews of our security practices.

Disclosure of Information: We disclose personally-identifiable information only to:
- Employees, contractors, and affiliated organizations who need it to process information on our behalf or provide services
- Comply with legal obligations or protect the rights, property, or safety of Anthropocene Alliance or the public

Some third parties may be located outside your home country. By using our website, you consent to such international data transfers. We do not sell or rent personally-identifying information. In the event of a merger or acquisition, user information may be transferred to the new entity.

Data Retention: We retain personally-identifiable information for as long as necessary to fulfill the purposes outlined in this policy, comply with legal obligations, or resolve disputes. Once this period ends, data will be securely deleted or anonymized.

Your Rights: You have the following rights regarding your personal data:
- Access and Correction: Request access to or correction of your information.
- Data Portability: Obtain a copy of your data in a portable format.
- Deletion: Request the deletion of your personal data, subject to legal or contractual limitations.
- Objection: Object to certain types of data processing, such as direct marketing.

To exercise these rights, please contact us at Info@AnthropoceneAlliance.org.

Children's Privacy: Our website is not intended for children under 13 years of age. We do not knowingly collect personal information from children. If we become aware of such data collection, we will delete it promptly.

Changes to the Privacy Policy: We may update this Privacy Policy from time to time. Significant changes will be communicated through our website or other appropriate means. Continued use of the website after changes are posted signifies your acceptance of the revised policy.

Donor Privacy

A2 is committed to protecting the privacy and confidentiality of our donors. This Donor Privacy Policy outlines how we collect, use, store, and protect the personal information of our donors in compliance with Florida's privacy laws, including the Florida Solicitation of Contributions Act and other applicable regulations.

Information We Collect: We may collect the following types of personal information when you make a donation to A2:

- Name
- Address
- Email address
- Phone number
- Payment information (credit card or bank details) via secure payment processors
- Donation history (amount, frequency, designated purpose, etc.)

We may also collect information from you when you engage with our website, sign up for newsletters, or participate in fundraising events.

How We Use Your Information: We use the personal information we collect to:

- Acknowledge and process your donation
- Send tax receipts and donor acknowledgments
- Communicate about our mission, programs, and fundraising activities (unless you opt out)
- Improve our outreach and services to our donors and supporters
- Comply with legal and regulatory requirements, including Florida's Solicitation of Contributions Act

We do not share or sell your personal information to third parties for marketing purposes.

How We Protect Your Information: We take your privacy seriously and have implemented security measures to protect your personal data. These measures include:

- Secure servers for storing donation information
- Encryption of sensitive payment data during transactions
- Restricting access to donor information to authorized personnel only

While we strive to protect your information, no method of transmission over the internet or electronic storage is completely secure. As such, we cannot guarantee absolute security but will continue to implement reasonable measures to safeguard your data.

Sharing Your Information: We respect your privacy and do not sell, trade, or rent your personal information to third parties. However, we may share information in the following circumstances:

- Service Providers: We may share your information with trusted third-party service providers that assist us with processing payments, sending emails, or other administrative functions.
- Legal Compliance: We may disclose your information if required to do so by law or in response to a legal request, such as a subpoena or court order, in accordance with Florida's legal requirements.
- With Your Consent: We may share your information with your consent, such as when you agree to have your name published in our donor recognition materials.

Florida-Specific Disclosures: In accordance with Florida law:

- Registration Requirements: As a Florida-based charity, we are required to be registered with the Florida Department of Agriculture and Consumer Services (FDACS) under the Florida Solicitation of Contributions Act. Our registration number is: CH61840. A copy of the official registration and financial information may be obtained from the FDACS, using the Check-A-Charity
- Public Disclosure: In accordance with Florida law, certain financial information regarding donations and our activities may be available to the public. If you wish to review or request our financial records, please contact us at the contact information above. Donors are entitled to request a copy of our latest financial report.

Opt-Out and Preferences: You have the right to opt out of receiving communications from us at any time. If you wish to unsubscribe from our newsletters or other marketing materials, you can do so by following the "unsubscribe" instructions provided in each communication or by contacting us directly at the contact information above.

Donor Recognition: If you choose to donate to the A2, we may recognize your contribution in our materials, such as annual reports, donor walls, or on our website. You may request to remain anonymous, and we will respect your wishes. If you prefer that your donation not be publicly recognized, please let us know when you make the donation.

Data Retention: We will retain your personal information for as long as it is necessary for the purposes outlined in this policy or as required by law. If you wish to have your information removed from our records, please contact us, and we will respond promptly.

Children's Privacy: A2 does not knowingly collect or solicit personal information from anyone under the age of 13. If you believe that we have inadvertently collected such information, please contact us so that we can take appropriate action.

Changes to This Privacy Policy: We may update this Donor Privacy Policy from time to time to reflect changes in our practices or legal obligations. When we make changes, we will update the "Effective Date" at the top of this page. We encourage you to review this policy periodically.

Whistle Blower

Purpose and Applicability: The purpose of these policies is to avoid, detect, and eliminate fraud and unlawful activity in all matters pertaining to A2. These policies apply to any

irregularity, or suspected irregularity, involving employees as well as Board members, contractors, and/or any other parties with a business relationship with A2.

Definition: Fraud is the use of deception or intentional misrepresentation to obtain an unjust or illegal financial or other advantage, or to avoid an obligation, or to cause loss to another party. The term includes theft, deception, bribery, forgery, fake documents, corruption, false accounting and conspiracy to commit these offences. Unlawful activity includes fraud and anything else that violate state, federal, and local law, and noncompliance with contracts and funding award agreements.

Duty: All staff and board members have a duty to familiarize themselves with the types of improprieties that might be expected to occur within their areas of responsibility and to be alert for any indications or irregularity. Anyone having reasonable suspicion of fraud or unlawful action on the part of another employee or the A2 as a whole must report them to their direct supervisor. In the event of suspicion regarding the direct supervisor, the report shall be made to the direct supervisor's supervisor. The collective Board is the supervisor of the Executive Director and individual Board members.

Investigation: The person receiving the report, in cooperation with the Executive Director or the Board will investigate suspected fraud and other unlawful activities. In the event that the allegation concerns the Executive Director, a board member, or A2 as a whole, an external investigator shall be used. Any investigative activity required will be conducted without regard to any person's relationship to A2, position or length of service. Reports of suspected unlawful activity will be kept confidential to the extent possible, consistent with the need to conduct an adequate investigation.

Consequence: If it is determined that unlawful activity has occurred or is occurring, the services of the party involved may be terminated. A2 will not retaliate against an employee in the terms and conditions of employment because that employee: (a) reports to A2 or a regulatory authority what the employee believes in good faith an unlawful activity; or (b) participates in good faith in any resulting investigation or proceeding, or (c) exercises their rights to take legal action.

IT and Data Policy

The purpose of this policy is to establish guidelines for the management, protection, and retention of data in alignment with the National Institute of Standards and Technology (NIST) standards. This policy aims to:

- Establish best practices for the use and management of IT resources.
- Ensure the confidentiality, integrity, and availability of organizational data.
- Mitigate risks associated with data breaches.
- Comply with relevant laws and regulations.

Scope: This policy applies to all data and IT resources collected, processed, transmitted, and stored by Anthropocene Alliance. It encompasses:

- IT systems, applications, and services used by the organization, including hardware, software, and cloud services.
- Electronic and physical data, including member information, employee records, financial data, intellectual property, and other organizational data assets.

Governance: This policy is implemented and enforced by the Chief Operations Officer.

Data Classification: Data shall be classified based on sensitivity, criticality, and regulatory requirements. Classification levels are:

- Sensitive Data: Information that could cause significant harm if disclosed, including personally identifiable information (PII), financial data, health records, and proprietary information.
- Internal Data: Information for internal use only, including operational data, internal communications, and non-sensitive intellectual property.
- External Data: Information intended for public consumption without sensitive or confidential details.

Data Handling Procedures

- Access Control: Implement the principle of least privilege, only those we require access are given it. Strong passwords and multi-factor authentication are required to ensure only authorized access.
- Data Storage: Store data in secure, encrypted systems that comply with NIST guidelines. Protect against unauthorized access, data loss, or theft.
- Data Transmission: Encrypt sensitive data during transmission to prevent unauthorized interception.
- Data Backup: Perform regular backups of critical data and store copies securely.
- Data Disposal: Securely dispose of data that is no longer required, rendering it irrecoverable through shredding or secure digital erasure.

Data Retention Periods

- Sensitive Data: Retain for 3 to 5 years as required by law or contractual obligations. Securely delete when no longer needed.
- Internal Data: Retain as necessary for operational needs. Securely delete when no longer required.
- External Data: Retain according to organizational policies and conduct regular reviews to remove outdated data.

Procurement Records

- Retain procurement records of transactions over $25,000 for five years post-final payment or conclusion of litigation/settlement.
- Retain other procurement documents for a minimum of three years after final payment or settlement conclusion.
- Retain subawardee files for three years post-final invoice submission.

Internal Data Governance Platforms. We use the following platforms:

- Social media (Facebook, LinkedIn, Instagram, YouTube) monitored via Hootsuite.
- EveryAction.
- Website designed with WordPress, hosted on Kinsta, domain registered with Dreamhost.
- Merchandise provider: Bonfire.
- Email provider: GoDaddy.
- Video conferencing: Zoom.
- Internal collaboration: AirTable.

All login information is stored in LastPass.

Security: Access to LastPass: Passwords and sensitive information are stored in LastPass. Chief Operations Officer, Senior Finance & Operations Manager, and IT Administrator are LastPass administrators. Finance-related access: Finance Advisor, Executive Director, Chief Operations Officer, Senior Finance & Operations Manager. Document storage on Google Shared Drive has specified access levels for all staff.

Financial Data: Our organization adheres to the Payment Card Industry Data Security Standard (PCI DSS) to ensure the secure handling of payment information. We use PureSight PureView as our payment processor, and the following measures are in place to maintain PCI compliance:

- Only designated personnel have access to the PureSight PureView account. Access is reviewed periodically and updated as necessary.
- Two-Factor Authentication (2FA): 2FA is enforced for all users accessing the PureSight PureView account to add an extra layer of security.
- Data Encryption: All payment card data is encrypted both in transit and at rest, ensuring secure transmission and storage of sensitive information.
- Regular Audits and Monitoring: We conduct regular security audits and monitor all access to cardholder data and the payment processor to detect and respond to any unauthorized activity.
- Employee Training: All staff handling payment information receive PCI compliance training to ensure they are aware of best practices for data security.
- Third-Party Compliance: We ensure that PureSight PureView is PCI DSS compliant and regularly verify their compliance status.

Employee Data Retention and Deletion: Upon an employee's departure or role change, their email account will be archived for a period of 1 year. During this time, all relevant emails and data will be moved to a designated archive folder. After 1 year, if the archived email account remains inactive, the information will be migrated to a long-term archive folder. The long-term archive folder will be securely stored and monitored for any necessary access.

The long-term archive folder will be monitored for access activity. If no access occurs within the next 6 months, the data will be flagged for deletion. After a total of 18 months (1 year of archiving and 6 months in the long-term archive folder), if the data remains unused, it will be securely deleted.

Password Management: We adhere to the following password management guidelines:

- Password Creation: Passwords must be a minimum of 12 characters long, and include a combination of uppercase and lowercase letters, numbers, and special characters.
- Avoid using easily guessable information such as birthdates, names, or common words.
- Consider using passphrases, which are longer and easier to remember.
- Password Protection: Do not share passwords with anyone under any circumstances.
- Avoid storing passwords in easily accessible locations, such as unsecured digital files.
- Utilize a reputable password manager to securely store and manage passwords.
- Authentication Methods: Implement an authenticator app, such as Google Authenticator, to enhance security. Authenticator apps generate one-time passcodes, adding an extra layer of protection during login. Some sites may offer passkeys for added security. If provided, securely store and follow the site's instructions on their usage.
- Password Rotation: Change passwords for all work-related accounts yearly. Email reminders will be sent to prompt timely password updates.

- Password Complexity: Avoid reusing passwords across multiple accounts. Ensure each password is unique and unrelated to personal information or previous passwords.

Web Security: The Web Security section outlines the measures and best practices to protect Anthropocene Alliance's online presence and web-based resources from security threats, including scams, phishing, and other cyber-attacks.

- Access Control: Implement strong authentication mechanisms for accessing web administrative interfaces, including multi-factor authentication (MFA).
- Enforce the principle of least privilege, granting access only to necessary personnel.
- Email Security: Implement email filtering solutions to detect and block phishing emails and other malicious messages. Use email authentication protocols such as SPF, DKIM, and DMARC to prevent email spoofing.
- Safe Browsing Practices: Use secure and up-to-date web browsers with built-in anti-phishing features. Verify the authenticity of websites before entering sensitive information and to avoid clicking on suspicious links.
- User Education: Conduct regular training sessions for employees on recognizing and avoiding phishing scams and other online threats.
- Distribute educational materials and updates about the latest phishing tactics and how to report suspicious activities.

AI Use: Anthropocene Alliance seeks to avoid the use of artificial intelligence (AI) in our writing, research and analysis. In these situations, we seek to follow responsible use of AI technologies while protecting data privacy, security, and integrity in alignment with the National Institute of Standards and Technology (NIST) standards. This includes AI for data analysis, decision-making, automation, and any other applications within the organization.

Do’s

- Ensure Transparency: Clearly document the purpose, function, and decision-making processes of AI systems.
- Data Privacy and Security: Use anonymized or pseudonymized data for AI training and processing wherever possible.
- Bias and Fairness: Note that AI models have biases. Take steps to mitigate any identified biases.
- Ethical Use: Use AI in a manner that aligns with our ethical guidelines and organizational values. Obtain informed consent from your direct supervisor when data is used for AI applications.
- Human Oversight: Ensure human oversight and the ability to intervene in AI-driven processes and decisions.
- Compliance: Ensure AI applications comply with relevant laws, regulations, and industry standards.

Don’ts

- Avoid Unethical Applications: Do not use AI for surveillance or monitoring of employees without proper authorization and transparency. Do not use AI in ways that could cause harm or discrimination against individuals or groups.
- Data Misuse: Do not use sensitive or personally identifiable information (PII) without proper authorization and consent. Avoid using data in ways that violate privacy agreements or organizational policies.

- Over-Reliance on AI: Do not rely solely on AI for critical decision-making without human validation.
- Lack of Transparency: Avoid implementing AI solutions without documenting the rationale, methodology, and expected outcomes.
- Neglecting Security Measures: Avoid using outdated or unpatched AI software that may be vulnerable to attacks.
- Ignoring Ethical and Legal Implications: Do not deploy AI applications that do not comply with ethical standards or legal requirements. Avoid using AI in jurisdictions where it may be restricted or regulated without ensuring compliance.

Security Audits: Regular audits and assessments will ensure compliance with this Data Policy and NIST standards. The policy will be reviewed and updated periodically to reflect technological, regulatory, or organizational changes. This procedure applies to all systems, applications, and services utilized by Anthropocene Alliance, specifically focusing on Google Workspace, Airtable, LastPass, and the A2 website.

Security audits will be conducted biannually (every six months) for the above-listed systems.

Google Workspace

- Access Control: Review user access permissions and ensure the principle of least privilege is enforced. Verify the use of multi-factor authentication (MFA) for all accounts.
- Data Protection: Ensure data encryption in transit and at rest. Verify the configuration of data loss prevention (DLP) policies.
- Activity Monitoring: Review audit logs for suspicious activities or unauthorized access attempts. Ensure logging and monitoring are enabled and properly configured.

Airtable

- Access Control: Review user roles and permissions to ensure appropriate access levels. Confirm the use of MFA for account access.
- Data Security: Ensure data encryption during storage and transmission. Verify the implementation of data backup and recovery procedures.
- Configuration Management: Review security settings and configurations for alignment with CIS controls. Validate that APIs and integrations follow secure coding practices.

LastPass

- Access Management: Review user access and administrative permissions. Ensure MFA is enforced for all accounts accessing LastPass.
- Data Security: Verify that all stored data is encrypted. Ensure secure sharing practices are followed for passwords and notes.
- Incident Response: Review incident response logs and past security incidents. Confirm the existence and effectiveness of incident response plans.

A2 Website

- Access Control: Review administrative access to the website’s backend. Verify the use of MFA for administrative accounts.
- Web Application Security: Conduct vulnerability scans to identify potential security flaws. Review the implementation of web application firewalls (WAFs) and secure coding practices.

- Data Protection: Ensure the encryption of data transmitted between users and the website. Verify the security of user data stored within the website's databases.
- Monitoring and Logging: Review web server and application logs for unusual or malicious activities. Ensure continuous monitoring and alerting systems are in place.

Reporting and Remediation

- Audit Report: Compile a detailed report summarizing the findings, including identified vulnerabilities, compliance gaps, and security weaknesses. Provide recommendations for remediation and enhancement of security controls.
- Remediation Plan: Develop and implement a remediation plan to address identified issues. Prioritize actions based on the severity and potential impact of the findings.
- Follow-up Audit: Conduct a follow-up audit to verify the implementation and effectiveness of remediation measures. Ensure continuous improvement by incorporating lessons learned into future audits.

Review and Update

- Policy Review: This Security Auditing Procedures document will be reviewed and updated annually or as required to reflect changes in technology, threats, or regulatory requirements.
- Continuous Improvement: Implement feedback from audits and incorporate industry best practices to enhance the effectiveness of security controls.

Incident Reporting: Report and address any incidents to the Operations and IT department

Employee Training: All employees, contractors, and third-party service providers must undergo comprehensive training on applicable information in this IT and Data Policy.

Compliance and Review: The policy will be reviewed and updated periodically to reflect technological, regulatory, or organizational changes.

Conflict of Interest

Purpose: The purpose of the conflict of interest policy (this "Policy") is to protect the interests of Anthropocene Alliance (the "Corporation") when it is contemplating entering into a transaction or arrangement that might benefit the private interests of an Officer, Director, employee or volunteer of the corporation or might result in a possible excess benefit transaction. This Policy is intended to supplement but not replace any applicable state and federal laws governing conflict of interest applicable to nonprofit and charitable organizations.

Definitions: In addition to the terms defined above and other terms defined in other Sections of this Policy, the following terms shall have the meanings set forth below for purposes of this Policy:

"Board" means, the Board of Directors of the Corporation.

"Family" means, an individual's brothers and sisters (whether by the whole or half blood or adoption), spouse, spouses of brothers or sisters (whether by whole or half blood or adoption), ancestors, children (including a legally adopted child), grandchildren, great-grandchildren, and

spouses of children, grandchildren and great-grandchildren (whether by whole or half blood or adoption).

“Interested Person” means, with respect to an entity or transaction, any Director, Officer, employee, or volunteer, who has a direct or indirect Financial Interest in that entity or transaction, as defined below.

“Financial Interest” means, a person or a Family member of that person has, directly or indirectly:

- An ownership or investment interest in any entity with which the Corporation has a transaction or arrangement,
- A compensation arrangement with the Corporation or with any entity or individual with which the Corporation has a transaction or arrangement, or
- A potential ownership or investment interest in, or compensation arrangement with, any entity or individual with which the Corporation is negotiating a transaction or arrangement.
- A material financial interest in or is engaged in some capacity in a business or enterprise that competes with the Corporation, or
- Received gifts, favors, gratuities or entertainment from a party who might be inferred to have provided such gifts, favors, gratuities or entertainment to influence the recipient in the performance of his or her duties. This does not preclude the acceptance of items of nominal or insignificant value or entertainment of nominal or insignificant value which are not related to any particular transaction of the Corporation.

For the purposes of this definition of a financial Interest, compensation includes direct and indirect remuneration as well as gifts or favors that are not insubstantial.

A Financial Interest is not necessarily a conflict of interest. A person who has a Financial Interest shall have a conflict of interest only if the Board or an appropriate committee decides that a conflict of interest exists.

Procedures: In connection with any actual or possible conflict of interest, an Interested Person must disclose the existence of the Financial Interest and be given the opportunity to disclose all material facts relating to each Financial Interest to the Directors to consider the proposed transaction or arrangement.

After disclosure of the Financial Interest and all material facts, and after any discussion with the Interested Person, he/she shall leave the Board or committee meeting while the determination of a conflict of interest is discussed and voted upon. The remaining Board members shall decide if a conflict of interest exists.

Procedures for Addressing the Conflict of Interest: An Interested Person may make a presentation at the Board or committee meeting, but after the presentation, he/she shall leave the meeting during the discussion of, and the vote on, the transaction or arrangement involving the possible conflict of interest.

The Chair of the Board or committee shall, if appropriate, appoint a disinterested person or committee to investigate alternatives to the proposed transaction or arrangement. After exercising due diligence, the Board or committee shall determine whether the Corporation can

obtain with reasonable efforts a more advantageous transaction or arrangement from a person or entity that would not give rise to a conflict of interest.

If a more advantageous transaction or arrangement is not reasonably possible under circumstances not producing a conflict of interest, the Board or committee shall determine by a majority vote of the disinterested Directors whether the transaction or arrangement is in the Corporation's best interest, for its own benefit, and whether it is fair and reasonable. In conformity with the above determination, it shall make its decision as to whether to enter into the transaction or arrangement.

Violations of the Conflicts of Interest Policy: If the Board or a committee has reasonable cause to believe a member of the Board or such committee has failed to disclose actual or possible conflicts of interest, it shall inform such member of the basis for such belief and afford such member an opportunity to explain the alleged failure to disclose.

If, after hearing such member's response and after making further investigation as warranted by the circumstances, the Board or committee determines such member has failed to disclose an actual or possible conflict of interest, it shall take disciplinary and corrective action as it shall deem appropriate under the circumstances.

Records of Proceedings: The minutes of the Board and all committees with Board delegated powers shall contain:

- The names of the persons who disclosed or otherwise were found to have a Financial Interest in connection with an actual or possible conflict of interest, the nature of the Financial Interest, any action taken to determine whether a conflict of interest was present, and the Board or committee's decision as to whether a conflict of interest in fact existed.
- The names of the persons who were present for discussions and votes relating to the transaction or arrangement, the content of the discussion, including any alternatives to the proposed transaction or arrangement, and a record of any votes taken in connection with the proceedings.

Compensation: A voting member of the Board who receives compensation, directly or indirectly, from the Corporation for services is precluded from voting on matters pertaining to that member's compensation.

A voting member of any committee whose jurisdiction includes compensation matters and who receives compensation, directly or indirectly, from the Corporation for services is precluded from voting on matters pertaining to that member's compensation.

No voting member of the Board whose jurisdiction includes compensation matters and who receives compensation, directly or indirectly, from the Corporation, either individually or collectively, is prohibited from providing information to any committee regarding compensation.

Annual Statements: Each Director and Officer shall annually sign a statement which affirms such person:

- Has received a copy of the Policy,
- Has read and understands the Policy,
- Has agreed to comply with the Policy, and

- Understands the Corporation is charitable and in order to be granted and maintain its federal tax exemption it must engage primarily in activities which accomplish one or more of its tax-exempt purposes.

Periodic Reviews: To ensure the Corporation operates in a manner consistent with charitable purposes and does not engage in activities that could jeopardize its tax-exempt status, periodic reviews shall be conducted by the Board or at the direction of the Board. The periodic reviews shall, at a minimum, include the following subjects:

- Whether compensation arrangements and benefits are reasonable, based on competent survey information, and the result of arm's length bargaining.
- Whether partnerships, joint ventures, and arrangements with management organizations conform to the Corporation's written policies, are properly recorded, reflect reasonable investment or payments for goods and services, further charitable purposes and do not result in inurement, impermissible private benefit or in an excess benefit transaction.

Use of Outside Advisors: When conducting the periodic reviews, the Corporation may, but need not, use outside advisors. If outside advisors are used, their use shall not relieve the Board of its responsibility for ensuring periodic reviews are conducted.