<div align="center">**Cottonwood, Inc.**
Policies and Procedures</div>

SECTION: Information Technology   **POLICY NO:** 07-007

SUBJECT: Artificial Intelligence (AI) Tool Usage

EFFECTIVE DATE: February 2024

Policy:

This Artificial Intelligence (AI) tool usage policy outlines best practices for use of artificial intelligence tools in the workplace, especially as it pertains to using sensitive data and proprietary company, consumer and customer information in these tools.

Scope:

Artificial intelligence (AI) tools have the potential to automate tasks, improve decision-making, and provide valuable insights into our operations.

However, the use of AI tools also presents new challenges in terms of information security and data protection. This policy is a guide for employees on how to be safe and secure when using AI tools, especially when it involves the sharing of potentially sensitive company, consumer and customer information.

Purpose:

The purpose of this policy is to ensure that all employees use AI tools in a secure, responsible and confidential manner. The policy outlines the requirements that employees must follow when using AI tools, including the evaluation of security risks and the protection of confidential data.

Policy Statement:

Cottonwood, Inc. recognizes that the use of AI tools can pose risks to our operations, consumers and customers. Therefore, we are committed to protecting the confidentiality, integrity, and availability of all company, consumer and customer data. This policy requires all employees to use AI tools in a manner consistent with our security best practices.

Security best practice:

All employees are expected to adhere to the following security best practices when using AI tools:

a. Evaluation of AI tools: The IT Department will evaluate the security of any AI tool before using it. This includes reviewing the tool's security features, terms of service, and privacy policy. The IT Department will also check the reputation of the tool developer and any third-party services used by the tool.

b. Protection of confidential data: Employees must not upload or share any data that is confidential, proprietary, or protected by regulation (HIPPA) without prior approval from the appropriate department director. This includes data related to customers, consumers, employees, or partners.

c. Access control: Employees must not give access to AI tools outside the company without prior approval from the appropriate director or management and subsequent processes as required to meet security compliance requirements. This includes sharing login credentials or other sensitive information with third parties.

d. Use of reputable AI tools: Employees should use only reputable AI tools approved by the IT Department. Any AI tool used by employees must meet our security and data protection standards.

e. Compliance with security policies: Employees must apply the same security best practices we use for all company and customer data. This includes using strong passwords, keeping software up-to-date, and following our data retention and disposal policies.

f. Data privacy: Employees must exercise discretion when sharing information publicly. Employees must ask themselves the questions, "Would I be comfortable sharing this information outside of the company? Would we be okay with this information being leaked publicly?" before uploading or sharing any data into AI tools. Second would be to follow b) above.

Review and revision:

This policy will be reviewed and updated on a regular basis to ensure that it remains current and effective. Any revisions to the policy will be communicated to all employees.

Conclusion:

Our organization is committed to ensuring that the use of AI tools is safe and secure for all employees and customers, as well as the organization itself. It's also crucial to remember that data entered into AI models might be stored and processed in ways that are beyond the company's immediate oversight and could potentially be accessed by external entities. We believe that by following the guidelines outlined in this policy, we can maximize the benefits of AI tools while minimizing the potential risks associated with their use.

Acknowledgement and compliance:

All employees must read and sign this policy before using any AI tools in the organization. Failure to comply with this policy may result in disciplinary action, up to and including termination.

By signing this policy, I acknowledge that I have read and understand the requirements outlined in this policy. I agree to use AI tools in a manner consistent with the security best practices outlined above and to report security incidents or concerns to the appropriate department director, IT department or management team member.

Employee Signature: _____

Date: _____