Jeeva AI, Inc.

Company Policy Packet

Last Revised: May 27, 2025

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Table of Contents

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Overview

The management of Jeeva AI, Inc. has implemented the information security policies outlined in this document. Jeeva AI, Inc.'s management team deems these policies essential to ensure confidential information is protected.

These policies set the direction, provide guidance, and demonstrate senior management support for the information security-related procedures across the organization.

Violation of policies within this manual may lead to in disciplinary action, which including suspension or employment termination. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may, at their discretion, report such activities to the applicable authorities.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Document Approvals

Policy Document	Jeeva AI, Inc. Company Policy Packet
Approver	Susy Pang
Approval Date	December 16, 2024
Next Review Date	December 16, 2025

Policy Document	Acceptable Use Policy
Approver	Susy Pang
Approval Date	December 9, 2024
Next Review Date	December 9, 2025

Policy Document	Asset Management Policy
Approver	Susy Pang
Approval Date	December 16, 2024
Next Review Date	December 16, 2025

Policy Document	Backup Policy
Approver	Susy Pang
Approval Date	November 20, 2024
Next Review Date	November 20, 2025

Policy Document	Business Continuity Plan
Approver	Susy Pang
Approval Date	December 8, 2024
Next Review Date	December 8, 2025

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Policy Document	Change Management Policy
Approver	Susy Pang
Approval Date	November 20, 2024
Next Review Date	November 20, 2025

Policy Document	Code of Conduct
Approver	Susy Pang
Approval Date	November 20, 2024
Next Review Date	November 20, 2025

Policy Document	Cryptography Policy
Approver	Susy Pang
Approval Date	November 20, 2024
Next Review Date	November 20, 2025

Policy Document	Data Classification Policy
Approver	Susy Pang
Approval Date	November 20, 2024
Next Review Date	November 20, 2025

Policy Document	Data Deletion Policy
Approver	Susy Pang
Approval Date	November 20, 2024
Next Review Date	November 20, 2025

Policy Document	Data Protection Policy
Approver	Susy Pang
Approval Date	December 8, 2024
Next Review Date	December 8, 2025

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Policy Document	Disaster Recovery Plan
Approver	Susy Pang
Approval Date	November 20, 2024
Next Review Date	November 20, 2025

Policy Document	Incident Response Plan
Approver	Susy Pang
Approval Date	November 20, 2024
Next Review Date	November 20, 2025

Policy Document	Information Security Policy
Approver	Susy Pang
Approval Date	November 20, 2024
Next Review Date	November 20, 2025

Policy Document	Password Policy
Approver	Susy Pang
Approval Date	November 20, 2024
Next Review Date	November 20, 2025

Policy Document	Responsible Disclosure Policy
Approver	Susy Pang
Approval Date	November 23, 2024
Next Review Date	November 23, 2025

Policy Document	Risk Assessment Program
Approver	Susy Pang
Approval Date	November 23, 2024
Next Review Date	November 23, 2025

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Policy Document	System Access Control Policy
Approver	Susy Pang
Approval Date	November 23, 2024
Next Review Date	November 23, 2025

Policy Document	Vendor Management Policy
Approver	Susy Pang
Approval Date	November 23, 2024
Next Review Date	November 23, 2025

Policy Document	Vulnerability Management Policy
Approver	Susy Pang
Approval Date	November 23, 2024
Next Review Date	November 23, 2025

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Jeeva AI, Inc. Acceptable Use Policy

Our customers trust us, and they expect us to protect the data and resources they've shared with us. Part of how we'll uphold that trust is through pre-established policies, so we don't need to make key decisions in critical moments.

Below, we explain the sections of our acceptable use policy: what each protects against, why a customer may care, and why we think each is important. We don't mean for the Acceptable Use Policy to intimidate, but we do aim for it to be clear.

Security and Proprietary Information

This section describes behaviors the company expects of you, including password hygiene and the use of multi-factor authentication.

Acceptable Use

The first part of this section details the consequences for malicious, negligent, and/or delinquent behavior. Neither intentionally harm others nor break laws.

The section's second part emphasizes that your employment by the company does not make you one of the company's public representatives. Instead, public communication and brand are controlled centrally at the company. While email and social media are mentioned specifically, please be conservative overall in how you represent yourself as an employee.

Policy Compliance

This section details the information security team's role in measuring, enforcing, and making exceptions to the policy and the potential consequences, including termination, for policy violations.

Acceptable Use Policy

1. Overview

Jeeva AI, Inc.'s intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Jeeva AI, Inc.'s established culture of openness, trust, and integrity. Instead, the team is committed to protecting Jeeva AI, Inc.'s employees, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP,

are the property of Jeeva AI, Inc. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is an organizational effort involving the participation and support of every employee and affiliate who deals with Jeeva AI, Inc. information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment when working for Jeeva AI, Inc. These rules are in place to protect the employee and Jeeva AI, Inc. Inappropriate use exposes Jeeva AI, Inc. to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to the use of information and network resources to conduct business or interact with internal networks and business systems, whether owned or leased by Jeeva AI, Inc., the employee, or a third party. All employees, contractors, consultants, temporary, and other workers, and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information and network resources in accordance with policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at Jeeva AI, Inc., including Jeeva AI, Inc.-affiliated personnel employed with third parties. This policy applies to all equipment that is owned or leased by Jeeva AI, Inc.

4. Policy

4.1 General Use and Ownership

4.1.1 Proprietary information stored on electronic and computing devices by the employee or a third party, remains the sole property of Jeeva AI, Inc. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Policy.

4.1.2 You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of proprietary information.

4.1.3 You may access, use, or share proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorized individuals within Jeeva AI, Inc. may monitor systems and network traffic at any time, per the company's auditing practices, details of which are documented in relevant technology and security-related policies.

4.1.6 Jeeva AI, Inc. reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with the Asset Management Policies.

4.2.2 Providing access to another individual, either deliberately or through failure to secure access, is prohibited.

4.2.3 Postings by employees from an email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Jeeva AI, Inc., unless posting is in the course of business duties.

4.2.4 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.2.5 Employees must use multi-factor authentication to authenticate to corporate accounts whenever available.

4.2.6 Employees must use a password manager to avoid insecure or shared passwords with accounts.

4.2.7 Employees must encrypt their devices if asked and must not interfere or otherwise reduce the level of encryption on their devices.

4.2.8 Employees must install OS updates onto their devices if asked or prompted. Employees should also be proactive about applying OS updates to their devices.

4.2.9 Employees must use antivirus software to protect the integrity and confidentiality of their laptops if asked and must not interfere or otherwise prohibit antivirus activities on their devices.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Jeeva AI, Inc. resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1 System and Network Activities: the following activities are strictly prohibited, in regard to work-related activities:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.

2. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

3. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

4. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

5. Using a computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

6. Making fraudulent offers of products, items, or services originating from any company account.

7. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

8. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes. Jeeva AI, Inc. Security team members providing pre-planned penetration testing and vulnerability scans on corporate

networks, infrastructure, and end user devices are exempt from this due to the nature of their job duties.

9. Port scanning or security scanning is expressly prohibited unless the Security team is notified in advance. Jeeva AI, Inc. Security team members providing pre-planned penetration testing and vulnerability scans on corporate networks, infrastructure and end user devices are exempt from this due to the nature of their job duties.

10. Executing any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's normal job/duty. Jeeva AI, Inc. Security team members providing pre-planned penetration testing and vulnerability scans on corporate networks, infrastructure and end user devices are exempt from this due to the nature of their job duties.

11. Circumventing user authentication or security of any host, network, or account. Jeeva AI, Inc. Security team members providing pre-planned penetration testing and vulnerability scans on corporate networks, infrastructure and end user devices are exempt from this due to the nature of their job duties.

12. Introducing honeypots, honeynets, or similar technology on the network.

13. Interfering with or denying service to any user other than the employee's host (for example, distributed denial of service (DDoS) attack).

14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

15. Providing information about, or lists of, employees to parties outside Jeeva AI, Inc.

4.3.2 Email and Communication Activities: Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company." Questions may be addressed to Jeeva AI, Inc. management.

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding “chain letters”, “Ponzi” or other “pyramid” schemes of any type.

6. Posting the same or similar non-business-related messages to large numbers of newsgroups or mailing lists (newsgroup spam).

7. Use of unsolicited email originating from within Jeeva AI, Inc.’s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by or connected via Jeeva AI, Inc.’s network.

4.3.3 Blogging and Social Media

1. Blogging by employees, whether using Jeeva AI, Inc.’s systems or personal systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Jeeva AI, Inc.’s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Jeeva AI, Inc.’s policy, is not detrimental to Jeeva AI, Inc.’s best interests, and does not interfere with an employee’s regular work duties. Blogging from Jeeva AI, Inc.’s systems is also subject to monitoring.

2. Employees are prohibited from revealing any confidential or proprietary information, trade secrets or any other material covered by Jeeva AI, Inc.’s Data Protection policy when engaged in blogging.

3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Jeeva AI, Inc. and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Jeeva AI, Inc.’s Code of Conduct.

4. Employees may also not attribute personal statements, opinions, or beliefs to Jeeva AI, Inc. when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly, or implicitly, represent themselves as an employee or representative of Jeeva AI, Inc. Employees assume any and all risk associated with blogging.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Jeeva AI, Inc.’s trademarks, logos and any other intellectual property may also not be used in connection with any blogging activity.

5. Policy Compliance

5.1 Compliance Measurement

The CFO will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the CFO in advance, and if applicable, documented in the Jeeva AI, Inc. Risk Register.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

- Asset Management Policy - Endpoints • Data Protection Policy
- Information Security Policy
- Password Policy
- Responsible Disclosure Policy • System Access Policy
- Code of Conduct

7. Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at https://www.sans.org/security-resources/glossary-of-terms/

- Blogging
- Honeypot
- Honeynet
- Proprietary Information
- Spam

Responsibility

The CFO is responsible for ensuring this policy is followed. Last updated: 12/09/2024

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Jeeva AI, Inc. Asset Management Policy: Endpoints Introduction

This Asset Management Policy is designed to protect customers' data stored on endpoints, including laptops and mobile devices. It details how Jeeva AI, Inc. accounts for endpoint information technology assets (e.g. employee computers) and outlines what should be done if assets are lost, destroyed, or otherwise damaged.

Asset Standards

The CFO must review and approve any new type of asset, computer model, that will be used for Jeeva AI, Inc.'s operations.

Currently, approved device manufacturer(s) include Apple, Acer, IBM ThinkPad's.

Devices should be configured such that there's reasonable confidence they will last 36 months.

Configuration Standards

When Jeeva AI, Inc. purchases the same hardware asset repeatedly, the team should design and implement consistent, secure configuration standards to ensure assets are configured securely and identically. The standards should be based on the team and role of the Jeeva AI, Inc. employee who will be using the asset.

Variations to the Configuration Standard

Deviations from the standard configuration should be documented and approved by the Jeeva AI, Inc.'s CFO. The CFO should only approve deviations for which there's a valid business need. Deviations will be documented in the company's inventory list.

Bring Your Own Device (BYOD) Policy:

Jeeva AI, Inc. employees can access company information using their own devices, including mobile devices. All employee-owned devices must conform to Jeeva AI, Inc. security policies if they're used to access Jeeva AI, Inc. data, systems, and/or IT infrastructure.

Asset Procurement Guidelines

Any request for Asset Procurement must be reviewed for compliance with Jeeva AI, Inc.'s Asset Standards by the company's CFO. Once the request passes review, the CFO is responsible for placing orders to procure the requested assets.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Software Licensing Guidelines

Jeeva AI, Inc.'s Vendor Management Policy details the policies for third-party software and services.

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. #{company} management will determine how serious an employee's offense is and take the appropriate action.

Responsibility

The CFO is responsible for ensuring this policy is followed.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Jeeva AI, Inc. Backup Policy

Jeeva AI, Inc.'s Backup Policy describes how often service and customer data is backed up. All original (non-derived) customer data on infrastructure operated by Jeeva AI, Inc. should be backed up.

Timing

Jeeva AI, Inc. configures full, daily database backups for all data stored for us by our cloud services provider. If a database instance is deleted, all associated backups are also automatically deleted.

Backups are periodically tested by the Jeeva AI, Inc. engineering team.

Endpoint Backups

Jeeva AI, Inc. does not maintain backups of employee endpoints (laptops or computers). Key tools, documents, and work products are expected to be stored on cloud services and shared file drives, so creating and maintaining backups of employee endpoints is not necessary.

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Jeeva AI, Inc. management will determine how serious an employee's offense is and take the appropriate action.

Responsibility

The CFO is responsible for ensuring this policy is followed.

Last updated: *11/20/2024*

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Jeeva AI, Inc. Business Continuity Policy

The following consists of a general Business Continuity Policy that represents governance of contingency plans for certain business-impacting outages and vendor disruption of service.

Business Continuity Policies

- Jeeva AI, Inc. performs testing of this Business Continuity Plan on an annual basis. The CEO is responsible for coordinating and conducting an annual rehearsal of this Business Continuity Plan.
- Whenever the BCP is enacted, it must be followed up with a retrospective in order to identify lessons learned and playbooks needing creation.
- Business Impact Assessments (BIA's) need to be conducted upon onboarding new, business-critical vendors. Please see the Vendor Management policy for more information and instructions.

Jeeva AI, Inc. Business Continuity Plan

The following consists of a general Business Continuity Plan for Jeeva AI, Inc. that represent vendor and service outages that could affect Jeeva AI, Inc. business operations, including contingency plans and workarounds. More detailed playbooks are available in Disaster Recovery Plan for infrastructure disasters.

This plan identifies key resources and needs to ensure that business may continue, perhaps in a limited capacity, in the event of a disaster.

The plan includes information such as key suppliers, contingency plans, and alternative business location.

Alternate Business Location

If Jeeva AI, Inc.'s primary work site is unavailable, an alternate work site shall be used by designated personnel. Jeeva AI, Inc.'s alternate work site is located at:

1603 Sage wood Way, San Marcos CA 92078

Personnel required to work at this alternate location are All remote.

Key Vendors - Contacts and Contingency Plans

Communications, Collaboration & SSO

Employees at Jeeva AI, Inc. communicate with customers over email and are equipped to engage customers in videoconferences or telephone calls. Jeeva AI, Inc. uses a Single Sign-On (SSO) provider for a number of business applications. If an outage is suspected with one of these systems, visit that system's status page. If no listed issue would explain the observed outage, submit a support ticket to the service provider through their support page.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Infrastructure - AWS

Jeeva AI, Inc.'s core business runs across different infrastructure offerings across AWS.

If an outage is suspected, visit the AWS status page at *https://status.aws.amazon.com* to see if there is a known issue. If no known issue is present or a possibility for Jeeva AI, Inc., submit a support ticket to AWS through their *support page*.

Jeeva AI, Inc. also has a support contact at AWS. In case of an outage or a suspected outage, please contact:

Michael Lin linmic@amazon.com

Please see the Jeeva AI, Inc. Disaster Recovery Plan for general and detailed action plans in case of various potential AWS outages and service disruptions.

Responsibility

The CEO is responsible for ensuring this policy is followed.

Appendix A: Insurance

Jeeva AI, Inc. has insurance in place in case of disruption or disaster. Insurance is through Marsh & McLennan Agency LLC with policy number D52772072, D52772084.

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Jeeva AI, Inc. management will determine how serious an employee's offense is and take the appropriate action.

Last updated: *12/8/2024*

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Jeeva AI, Inc. Change Management Process and Standard - Code Deployments

Jeeva AI, Inc.'s Change Management Policy describes how changes to the Jeeva AI, Inc. system are proposed, reviewed, deployed, and managed. This policy covers all changes made to the Jeeva AI, Inc. software, regardless of their size, scope, or potential impact.

This policy is designed to mitigate the risks of:

- corrupted or destroyed information
- degraded or disrupted computer performance
- productivity losses
- introduction of new vulnerabilities, configuration errors and software bugs in infrastructure and code
- exposure to reputation risk

Version Control

All of our software is version controlled and synced between contributors (developers). Access to the central repository is restricted based on an employee's role.

Using a decentralized version control system allows multiple developers to work simultaneously on features, bug fixes, and new releases; it also allows each developer to work on their own local code branches in a local environment.

All code is written, tested, and saved in a local repository before being synced to the origin repository. Writing code locally decouples the developer from the production version of our code base and insulates us from accidental code changes that could affect our users. In addition, any changes involving the persistence layer (database) are performed locally when developing new code, where errors or bugs can be spotted before the change is deployed to users.

Branching Model

Production branch:

The prodbranch reflects the current state of the application in production.

Staging branch

The devbranch reflects the current state of the application on the staging server.

Development branch

The devbranch reflects the development changes delivered most recently for the next release.

Feature branches

Feature branches are used to develop new features for a future release, the specifics of which might not be known when development starts. A given feature branch will exist as long as the feature

Is in development, the branch will eventually either be merged back into dev, to add the new feature to an upcoming release with a pull request or discarded (if the feature will not be added to an upcoming release). Feature branches may branch off from and must merge back into dev. They typically exist in developer repos only, not in origin.

Security bugs

Jeeva AI, Inc. recognizes that security bugs represent key issues that should be resolved quickly to maintain the security, confidentiality, privacy, processing integrity, and availability of the service. Jeeva AI, Inc. commits to resolving security bugs within reasonable timelines as outlined by company procedural commitments in Vanta.

Hotfix branches

Hotfix branches are meant for new, unplanned production releases that address the live system being in an undesired state. A hotfix branch is made off of the master branch, with the latest production version, when a critical production bug must be resolved. This allows team members on the master branch to continue their work while someone else prepares the bug fix.

When finished, the bug fix needs to be merged back into the original branch, so it is deployed to production. The merge should be done through a pull request.

Hotfixes that are merged directly into prod, without going through dev, are exceptions that should be used only when a critical bug in the production system needs to be addressed immediately.

Permission for a hotfix should be obtained from the engineering leadership and should be noted in the pull request.

Change Initiation

To initiate a change, the developer first creates a feature branch on his or her local machine. Code changes are grouped into diffs, each of which represents a proposed change to the codebase.

Pull Requests

When a developer finishes a feature branch, they make a pull request to merge those changes into master. This submits the changes for peer review. For all code changes, the reviewer should be different from the author.

Pull requests allow developers to describe the changes they're making; co-workers can review the set of changes in a code review. Pull requests also trigger automated testing and code-quality checks that must be completed and returned successfully before merging is allowed. Testing and approval are logged by the system.

A pull request's details section should be used to note any non-code changes (e.g. environment or database changes) needed before the commits are merged.

Once tests pass and the code is approved, the author can merge the code to the central repository.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Merging a Pull Request

Before merging a pull request, the developer should check that all prerequisites have been met, including environment changes or database migrations. Once non-code changes have been implemented, the pull request can be merged.

If the application is deployed through our standard, zero-downtime development process, the developer's job is complete.

If any of these changes necessitate system down-time, the merge should take place within a scheduled and pre-announced window when customers are less likely to be affected.

Code Reviews, Change Review, and Change Approval

Before the feature branch is merged, a code review should be performed. Code reviews are performed by a second developer (i.e. not the one who wrote the code), who considers questions like:

- Are there any obvious logic errors in the code?
- Are all cases specified in the requirements fully implemented?
- Is there sufficient automated testing for the new code? Do existing automated tests need to be rewritten to account for code changes?
- Does the new code conform to existing style guidelines?
- Are there any egregious security errors as defined by the *OWASP Top 10* ?

A code review should take place after all code has been written and automated tests have been run and passed, as this ensures the reviewer's time is spent checking what automation misses.

The reviewer should note all potential issues with the code; it is the responsibility of the author(s) to address those issues or explain why they are not applicable.

Once the review process finishes, each reviewer should leave a comment on the pull request confirming the change is accepted and approve the entire pull request. Only when the pull request is accepted may the original author(s) may merge their change into the release branch.

Automated Testing

When a pull request is initiated, our automated test suite is triggered to run against the new code.

Deployment

The system is monitored on a continuous basis. Should the site be negatively affected by a change, that code change is rolled back.

Zero Downtime Deployment

Zero-downtime deployments allow us to make changes without waiting for a change window and allow us to return the application to a previous state easily.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Jeeva AI, Inc. management will determine how serious an employee's offense is and take the appropriate action.

Responsibility

The CFO is responsible for ensuring this policy is followed.

Last updated: *11/20/2024*

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Jeeva AI, Inc. Employee Code of Conduct

Purpose

The primary goal of Jeeva AI, Inc.'s Code of Conduct is to foster inclusive, collaborative, and safe working conditions for all Jeeva AI, Inc. staff. As such, Jeeva AI, Inc. are committed to providing a friendly, safe, and welcoming environment for all staff, regardless of gender, sexual orientation, ability, ethnicity, socioeconomic status, and religion (or lack thereof).

This code of conduct outlines our expectations for all Jeeva AI, Inc. staff, as well as the consequences for unacceptable behavior.

Scope

Jeeva AI, Inc. Code of Conduct applies to all Jeeva AI, Inc. staff. This includes full-time, part-time and contractor staff employed at every seniority level. The Code of Conduct is to be upheld during all professional functions and events, including but not limited to business hours at the Jeeva AI, Inc., extracurricular activities, and events, while attending conferences and other professional events on behalf of Jeeva AI, Inc., and while working remotely and communicating on Jeeva AI, Inc. resources with other staff.

We expect all Jeeva AI, Inc. staff to abide by this Code of Conduct in all business matters – online and in-person – as well as in all one-on-one communications with customers and staff pertaining to Jeeva AI, Inc. business.

This Code of Conduct also applies to unacceptable behavior occurring outside the scope of business activities when such behavior has the potential to adversely affect the safety and well-being of Jeeva AI, Inc. staff and clients.

Jeeva AI, Inc. Culture & Citizenship

A supplemental goal of this Code of Conduct is to increase open citizenship by encouraging participants to recognize the relationships between our actions and their effects within Jeeva AI, Inc. culture.

Be welcoming. We strive to be a company that welcomes and supports people of all backgrounds and identities. This includes, but is not limited to members of any race, ethnicity, culture, national origin, color, immigration status, social and economic class, educational level, sexual orientation, gender identity and expression, age, size, family status, political belief, religion, and mental and physical ability.

Be considerate. Your work at Jeeva AI, Inc. will be used by other people, and you in turn will depend on the work of others. Any decision you take will affect users and colleagues, and you should take those consequences into account when making decisions.

Be respectful. Not all of us will agree all the time, but disagreement is no excuse for poor behavior and poor manners. We might all experience some frustration now and then, but we cannot allow that frustration to turn into a personal attack. It's important to remember that a company where people feel uncomfortable or threatened is neither productive nor pleasant. Jeeva AI, Inc. staff should always be respectful when dealing with people outside of Jeeva AI, Inc. employment.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Acceptable and Expected Behavior

The following behaviors are expected and requested of all Jeeva AI, Inc. staff:

- Participate in an authentic and active way. In doing so, you contribute to the health and longevity of Jeeva AI, Inc.
- Exercise consideration and respect in your speech and actions at all times.
- Attempt collaboration before conflict.
- Refrain from demeaning, discriminatory, or harassing behavior and speech.
- Be mindful of your surroundings and of your fellow participants. Alert Jeeva AI, Inc. leaders if you notice a dangerous situation, someone in distress, or violations of this Code of Conduct, even if they seem inconsequential.
- Remember that Jeeva AI, Inc. events may be shared with members of the public and Jeeva AI, Inc. customers; please be respectful to all patrons of these locations at all times.

Unacceptable Behavior

The following behaviors are considered harassment and are unacceptable within our community:

- Violence, threats of violence or violent language directed against another person.
- Sexist, racist, homophobic, transphobic, ableist or otherwise discriminatory jokes and language.
- Posting or displaying sexually explicit or violent material.
- Posting or threatening to post other people's personally identifying information ("doxing").
- Personal insults, particularly those related to gender, sexual orientation, race, religion, or disability. Inappropriate photography or recording.
- Inappropriate physical contact. You should have someone's consent before touching them in any manner.
- Unwelcome sexual attention. This includes sexualized comments or jokes, inappropriate touching, groping, and unwelcome sexual advances.
- Deliberate intimidation, stalking or following (online or in person).
- Advocating for, or encouraging, any of the above behavior.
- Repeated harassment of others. In general, if someone asks you to stop, then stop.

Weapons Policy

No weapons will be allowed at Jeeva AI, Inc. events, office locations, or in other spaces covered by the scope of this Code of Conduct. Weapons include but are not limited to guns, explosives (including fireworks), and large knives such as those used for hunting or display, as well as any other item used for the purpose of causing injury or harm to others. Anyone seen in possession of one of these items will be asked to leave immediately and will be subject to punitive action up to and including termination and involvement of law enforcement.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Consequences of Unacceptable Behavior

Unacceptable behavior from any Jeeva AI, Inc. staff, including those with decision-making authority, will not be tolerated.

Anyone asked to stop unacceptable behavior is expected to comply immediately.

If a staff member engages in unacceptable behavior, Jeeva AI, Inc. leadership may take any action deemed appropriate, up to and including suspension or termination.

Reporting Violations

If you are subject to or witness unacceptable behavior, or have any other concerns, please notify an appropriate member of Jeeva AI, Inc. leadership as soon as possible.

It is a violation of this policy to retaliate against any person making a complaint of Unacceptable Behavior or against any person participating in the investigation of (including testifying as a witness to) any such allegation. Any retaliation or intimidation may be subject to punitive action up to and including termination.

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Jeeva AI, Inc. management will determine how serious an employee's offense is and take the appropriate action.

Responsibility

It is the CEO's responsibility to ensure this policy is followed.

Credits

Policy created from the following Open-Source Codes of Conduct text and guidance.

Last updated: *11/20/2024*

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Jeeva AI Supplier Code of Conduct

This Supplier Code of Conduct sets forth the minimum standards and expectations for all suppliers, vendors, contractors, and their subcontractors ("Suppliers") who conduct business with Jeeva AI, Inc. Jeeva AI, Inc. is committed to upholding the highest standards of ethical, legal, and responsible business practices, particularly in the rapidly evolving field of artificial intelligence. This Code is designed to ensure that all Suppliers align with Jeeva AI's values and comply with applicable laws, regulations, and best practices.

Legal and Regulatory Compliance

- Suppliers must comply with all applicable international, national, and local laws, regulations, and standards in every jurisdiction where they operate. This includes, but is not limited to, laws relating to labor, human rights, health and safety, the environment, intellectual property, data protection, trade controls, antitrust, and anti-corruption.
- Suppliers must implement robust compliance programs, including policies, procedures, training, and internal controls, to ensure ongoing adherence to legal requirements.

Ethical Business Practices

- Suppliers must conduct business with integrity, transparency, honesty, and fairness in all dealings.
- All forms of corruption, bribery, extortion, and embezzlement are strictly prohibited. Suppliers must not offer or accept bribes or other improper incentives.
- Conflicts of interest must be disclosed and managed appropriately.
- Suppliers must maintain accurate and transparent business records and cooperate fully with regulatory authorities or Jeeva AI's audits.

Labor and Human Rights

- Suppliers must uphold the fundamental human rights of workers and treat them with dignity and respect.
- Forced labor, bonded labor, indentured labor, prison labor, and child labor are strictly prohibited. All employment must be voluntary, and workers must be free to leave after reasonable notice.
- Suppliers must comply with minimum age laws and verify the age and legal status of all workers.
- Discrimination or harassment based on race, color, gender, age, sexual orientation, disability, religion, political affiliation, or any other protected characteristic is prohibited.
- Workers must be provided with safe and healthy working conditions, fair wages, reasonable working hours, and the right to freedom of association.

Environmental Responsibility

- Suppliers must comply with all applicable environmental laws and regulations and strive to minimize their environmental impact.
- Responsible sourcing of materials, reduction of waste, proper management of hazardous substances, and efforts to reduce carbon footprint are expected.
- Suppliers should work towards sustainable practices in their operations and supply chains.

Health and Safety

- Suppliers must provide a safe and healthy workplace for their employees, complying with all applicable health and safety laws and regulations.
- Adequate policies and procedures must be in place to prevent accidents, injuries, and exposure to health

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

risks.

Data Protection, Confidentiality, and Intellectual Property

- Suppliers must protect all confidential and proprietary information belonging to Jeeva AI and its clients, using it only as authorized and taking steps to prevent unauthorized disclosure or misuse.
- Suppliers must comply with all applicable data protection and privacy laws, especially when handling personal data or sensitive information.
- Intellectual property rights of Jeeva AI and third parties must be respected at all times.

AI-Specific Requirements

- Suppliers providing AI-related products or services must comply with all relevant AI regulations (such as the EU AI Act), including bias audits, transparency, and documentation requirements.
- Comprehensive documentation of data sources, model development, and deployment processes must be maintained and made available for review upon request.
- Suppliers are expected to have clear policies for mitigating bias, ensuring fairness, and addressing ethical concerns in AI systems.
- Robust cybersecurity measures must be in place to protect AI models and data from threats such as data poisoning, prompt injection, and model theft.

Monitoring, Auditing, and Continuous Improvement

- Jeeva AI reserves the right to monitor and audit Supplier compliance with this Code, including on-site inspections and review of relevant documentation.
- Suppliers must promptly address any identified non-compliance and implement corrective actions as required.
- Suppliers are encouraged to continuously improve their practices, leveraging technology (such as AI-driven compliance monitoring) to proactively manage risks and enhance compliance.

Reporting and Whistleblower Protection

- Suppliers must provide a mechanism for employees and stakeholders to report concerns or violations of this Code without fear of retaliation.
- All reports must be investigated promptly and thoroughly, and appropriate corrective actions must be taken.

Consequences of Non-Compliance

- Failure to comply with this Supplier Code of Conduct may result in corrective action, suspension, or termination of the business relationship with Jeeva AI.

By conducting business with Jeeva AI, Suppliers acknowledge and agree to comply with the standards and requirements set forth in this Supplier Code of Conduct. This Code is subject to periodic review and may be updated by Jeeva AI to reflect evolving laws, regulations, and best practices.

Responsibility

It is the CEO's responsibility to ensure this policy is followed.

Last updated: 11/20/2024

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Jeeva AI, Inc. Encryption & Key Management Policy

This policy provides guidance to limit encryption to those algorithms that have received substantial public review and have been proven to work effectively.

Additionally, this policy document provides Jeeva AI, Inc. encryption standards and best practices to ensure that Jeeva AI, Inc. consistently follows industry standards for Encryption and Key Management.

This policy and standard applies to all Jeeva AI, Inc. employees, contractors, and third-party vendors when sensitive data, such as customer data, Jeeva AI, Inc. secrets and PII, are in scope.

Data Encryption Policy

- All sensitive data in transit and at rest must be encrypted using strong, industry-recognized algorithms.
- Jeeva AI, Inc. maintains approved encryption algorithm standards. These internal standards are reviewed and subject to change when significant changes to encryption standards within the security industry change.
- Jeeva AI, Inc. will not engage in "roll-your-own" encryption, algorithms, or practices and will not use "security through obscurity" within production infrastructure or applications.
- All Jeeva AI, Inc.-owned, employee-utilized computers are to have full disk encryption enabled at all times, as these devices are expected to interact with Jeeva AI, Inc. resources, infrastructure and/or client data while performing Jeeva AI, Inc. business.

AWS Data Encryption

Jeeva AI, Inc. uses AWS resources to store and encrypt sensitive data. To keep data encrypted at rest, Jeeva AI, Inc. ensures that all new and existing resources use Amazon server-side encryption. By default, AWS encryption uses AWS-owned or AWS-managed keys stored in KMS or S3. Specific services can also be configured to use customer-managed encryption keys using KMS or customer-supplied encryption keys.

Amazon server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt Jeeva AI, Inc. data.

Jeeva AI, Inc. engineers are required to ensure that Amazon resources are correctly configured to use AWS server-side encryption in a secure manner following Amazon recommendations.

Data in Transit

- The minimum acceptable TLS standard in use by the company is TLS v1.2.
- All Jeeva AI, Inc. public web properties, applicable infrastructure components and applications using SSL/TLS, IPSEC and SSH to facilitate the encryption of data in transit over open, public networks, must have certificates signed by a known, trusted provider.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Jeeva AI, Inc. Encryption Standards

The CFO is responsible for reviewing all encryption algorithms in use. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the *IETF/IRTF Cipher Catalog*, or the set defined for use in the United States National Institute of Standards and Technology *(NIST) publication FIPS 140-2* , or any superseding documents according to the date of implementation.

Algorithms in use must meet the standards defined for use in *NIST publication FIPS 140-2* or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.

Jeeva AI, Inc. Encryption Key Creation & Storage Standards

Encryption Keys generated, stored, and managed by Jeeva AI, Inc.

- Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.
- Key generation must be seeded from an industry standard random number generator (RNG). For examples, see *NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2*.

Auditing

The CFO will verify compliance to this policy through various methods, including but not limited to code reviews, periodic infrastructure, and database reviews, Vanta platform monitoring, and internal and external audits. Feedback will be provided to the appropriate Jeeva AI, Inc. team(s) upon completion of audits and reviews if remediation is required.

Exceptions

Any exception to the policy must be approved by the CFO in advance and placed on a risk register for monitoring and periodic review.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including employment termination.

Responsibility

The CFO is responsible for ensuring this policy is followed.

Last updated: *11/20/2024*

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Jeeva AI, Inc. Data Classification Policy

In order to effectively secure Jeeva AI, Inc.'s data, staff must have a shared vocabulary to describe the data and the corresponding protection it requires. This policy describes how company data is classified and the levels of protection required for each classification.

Data Classification Standards

All Jeeva AI, Inc. information and all information entrusted to Jeeva AI, Inc. from third parties falls into one of four classifications, in order of increasing sensitivity.

Category	Description	Examples
Public	Public information is not coni- denial and can be made public without any implications for In- volve ai.	• Press releases • Public website
Internal	Access to internal information is approved by management and is protected from external access.	• Internal memos • Design documents • Product specifications • Correspondences
Customer confidential	Information received from customers for processing or storage by Jeeva AI, Inc. Jeeva AI, Inc. must up- hold the highest possible levels of integrity, confidentiality, and restricted availability for this in- formation.	• Customer operating data • Customer PII • Customers' customers' PII • Anything subject to a confidentiality agreement with a customer
Company confidential	Information collected and used by Jeeva AI, Inc. to operate the business. Jeeva AI, Inc. must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Legal documents • Contractual agreements • Employee PII • Employee salaries

Public

Public data is information that may be disclosed to any person regardless of their affiliation with Jeeva AI, Inc. The "public" classification is not limited to data that is of public interest or intended to be distributed to the public; the classification applies to any data that does not require any level of protection from disclosure. While it might be necessary to protect original (source) documents from unauthorized modification, public data may be shared with a broad audience both within and outside Jeeva AI, Inc., and no steps need be taken to prevent its distribution.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Internal

Internal data is information that is potentially sensitive and should not be shared with the public. Internal data generally should not be disclosed outside of Jeeva AI, Inc. without the permission of Jeeva AI, Inc. management. It is the responsibility of the data owner to designate information as internal where appropriate.

Unauthorized access has the potential to influence Jeeva AI, Inc.'s operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence.

Customer Confidential

Customer-confidential data is information that, if made available to unauthorized parties, may adversely affect Jeeva AI, Inc. customers. This classification also includes data that Jeeva AI, Inc. is required to keep confidential, either by law or under a confidentiality agreement with non-customer third parties, such as vendors. This information is to be protected against unauthorized disclosure or modification. Customer-confidential data should be used only when necessary for business purposes with the permission of the customer and should be protected both when it is in use and when it is being stored, processed, or transmitted.

Unauthorized access has the potential to influence Jeeva AI, Inc.'s operational effectiveness, violate contractual confidentiality agreements, initiate a security incident, or cause a major drop in both customer and industry confidence.

Company Confidential

Company-confidential data is information that, if made available to unauthorized parties, might adversely affect Jeeva AI, Inc. This information is to be protected against unauthorized disclosure or modification, and might be limited to executives, HR, and legal parties employed by or under contract with Jeeva AI, Inc. Company-confidential data should be used only by pre-authorized parties and should be protected both when it is in use and when it is being stored, processed, or transmitted. Unauthorized access has the potential to influence Jeeva AI, Inc.'s operational effectiveness, violate contractual confidentiality agreements, initiate a security incident, or cause a major drop in employee, customer, and industry confidence.

Scope

This data classification standard and policy is to be applied to all Jeeva AI, Inc. data, both physical and electronic. No data item is too small to be classified.

Policy

- Jeeva AI, Inc. managers or information owners shall be responsible for assigning classifications to information assets according to Jeeva AI, Inc. Data Classification Standards.
- Whenever possible, clearly label each piece of information with its data classification.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Non-Compliance

Since classifying data is an important part of protecting data and systems for Jeeva AI, Inc., employees who purposely violate this policy are subject to disciplinary action up to and including denial of access, legal penalties, and/or dismissal. Any employee aware of any violation of this policy is required to report it to their supervisor or other authorized representative.

Responsibility

The CFO is responsible for communicating and upholding the Data Classification Policy and Standards.

All staff are responsible for following the Data Classification Policy and Standards.

Last updated: *11/20/2024*

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Jeeva AI, Inc. Data Deletion Policy

Jeeva AI, Inc.'s Data Deletion Policy describes how customer data is deleted in connection with the cancellation or termination of a Jeeva AI, Inc. account.

This policy applies to all data collected by Jeeva AI, Inc. except:

- data that resides in any Jeeva AI, Inc. product or service not covered by this policy
- data that resides in third-party services managed and hosted by third parties, with the exception of the company's infrastructure provider
- data that resides in Jeeva AI, Inc. products or services that are in beta, testing, or an early access program

By default, a customer's data is stored for the duration of his or her contract with Jeeva AI, Inc.

The data may be deleted within one month after the contract ends, at the latest, with the exception of data that is required to establish proof of a right or a contract, which will be stored for the duration provided by enforceable law.

Once deleted, a user's data cannot be restored.

Jeeva AI, Inc. may provide the option for customers to delete data after their subscription ends. This request must be made by the customer, and Jeeva AI, Inc. may require additional ID verification. Jeeva AI, Inc. should hard delete all information from currently running production systems within one month of the deletion request.

Only the following employees can delete customer data in the event that Jeeva AI, Inc. is required to do so:

- Chief Technology Officer
- Technical Lead
- DevOps Manager

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Jeeva AI, Inc. management will determine how serious an employee's offense is and take the appropriate action.

Responsibility

It is the responsibility of the CFO to manage the list of team members that may handle customer requests for data deletion.

The CFO is responsible for ensuring this policy is followed.

Last updated: *11/20/2024*

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Jeeva AI, Inc. Data Protection Policy

Introduction

This policy refers to all data collected from employees, candidates, users, customers, vendors, or other parties that provide information to Jeeva AI, Inc.

Jeeva AI, Inc. employees must follow this policy. Contractors, consultants, partners, and any other external entities are also covered. Generally, our policy refers to anyone we collaborate with or who acts on our behalf and may need access to Jeeva AI, Inc. data.

Data Protection Policy

As part of our operations, we obtain and process information, some of which can be used to identify individuals (personally identifiable information, or PII).

Our company collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

The data will be:

- Accurate and kept up to date
- Collected fairly and for lawful purposes only
- Processed by the company within its legal and ethical boundaries
- Protected against any unauthorized or illegal access by internal and external parties

The data will not be:

- Communicated informally
- Stored for more than the amount of time specified in our Terms of Service, Privacy Policy, customer contracts, or other binding agreements
- Transferred to organizations, states, or countries that do not have adequate data protection policies
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

In addition to ways of handling the data, Jeeva AI, Inc. has direct obligations towards people to whom the data belongs. Specifically, we must:

- Inform people about who has access to their information
- Have provisions in cases of lost, corrupted, or compromised data
- Allow people to request that we modify, erase, reduce, or correct data contained in our databases within legal guidelines specified by company policies or law-enforcement agencies

To exercise data protection, we're committed to:

- Restrict and monitor access to sensitive data

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

- Develop transparent data collection procedures
- Train employees in online privacy and security measures
- Build secure networks to protect online data from cyberattacks
- Establish clear procedures for reporting privacy breaches or data misuse
- Include contract clauses or communicate statements on how we handle data
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Jeeva AI, Inc. management will determine how serious an employee's offense is and take the appropriate action.

Other Information

Currently, approved device manufacturer(s) include Apple, Acer, IBM ThinkPad's

Further Questions and Responsibility

Any questions regarding the use of or suggested modifications to Non-Disclosure Agreements should be referred to the Operations team.

It is the Operations team's responsibility for ensuring this policy is followed.

Last updated: *11/24/2024*

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Jeeva AI, Inc. Disaster Recovery Plan

The Jeeva AI, Inc. Disaster Recovery Plan ("DRP") establishes procedures to recover Jeeva AI, Inc. operations following a disruption resulting from a disaster. The types of disasters contemplated by this plan include natural disasters, political disturbances, man-made disasters, external human threats, and internal malicious activities. This DRP is maintained by the Operations team.

Disaster Recovery Policies

- Jeeva AI, Inc. performs testing of the Disaster Recovery Plan annually. The Operations team is responsible for coordinating and conducting rehearsals of this Disaster Recovery Plan annually.
  - Whenever the DRP is used, it must be followed by a retrospective and tabletop reenactment in order to identify lessons learned and playbooks needing creation.
- This policy and plan must be updated at least annually with additional playbooks considering new risks of disasters learned through testing and reenactment of past disaster incidents.

Scope of Disaster Recovery Plan

This policy includes all resources and processes necessary for service and data recovery and covers all information security aspects of business continuity management.

The following conditions must be met for this plan to be viable:

1. All equipment, software, and data (or their backups/failovers) are available in some manner.
2. If an incident takes place at the organization's physical location, all resources involved in recovery efforts are able to be transferred to an alternate work site (such as their home office) to complete their duties.

This plan does not cover the following types of incidents:

1. Incidents that affect customers or partners but have no effect on Jeeva AI, Inc.'s systems. In this case, the customer must employ their own continuity processes to make sure that they can continue to interact with Jeeva AI, Inc. systems.
2. Incidents that affect cloud infrastructure suppliers at the core infrastructure level, including but not limited to Google, Slack, and Amazon Web Services. The organization depends on such suppliers to employ their own continuity processes.

Notification List

In the event of a disaster, notify these people in order:

- Gaurav Bhattacharya, CEO, gaurav@jeeva.ai
- Susanna Pang, CFO, susy@jeeva.ai

Disaster Recovery Objectives

The objectives of this plan are the following:

- Identify the activities, resources, and procedures needed to carry out Jeeva AI, Inc.'s processing requirements during prolonged interruptions to normal operations.
- Identify and define the impact of interruptions to Jeeva AI, Inc.'s systems.
- Assign responsibilities to designated personnel and provide guidance for recovering Jeeva AI, Inc. operations during prolonged periods of interruption to normal operations.
- Ensure coordination with other Jeeva AI, Inc. staff who will participate in the contingency planning strategies.
- Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies. Please see Jeeva AI, Inc.'s critical contacts on Jeeva AI, Inc.'s Business Continuity Plan.

Defining Critical Systems and Services

From a disaster recovery perspective, Jeeva AI, Inc. defines two categories of systems:

Non-Critical Systems. These are all systems not considered critical by the definition below. These systems, while they may affect the performance and overall security of Critical Systems, do not prevent Critical Systems from functioning and being accessed appropriately. Non-Critical Systems are restored at a lower priority than Critical Systems. Examples of Non-Critical Systems include analytics servers.

Critical Systems. These systems host application servers and database servers or are required for the functioning of systems that host application servers and database servers. These systems, if unavailable, affect the integrity of data and must be restored, or have a process begun to restore them, immediately upon becoming unavailable.

The following services and technologies are considered to be critical for Jeeva AI, Inc. business operations, and must immediately be restored (in priority order):

1. Production infrastructure
2. Transit infrastructure
3. Build and deployment infrastructure

General Disaster Recovery Plan

While specific playbooks are available for specific scenarios, there are overall rules of engagement whenever a disaster incident needs to be opened.

Notification Phase

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to Jeeva AI, Inc. The notification sequence is listed below:

1. The first person to report the disaster should notify Gaurav Bhattacharya.
2. Gaurav Bhattacharya is to notify team members referenced above in the Notification List section.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

3. Based on the damage assessment, if Jeeva AI, Inc. will be unavailable to customers for more than 24 hours Gaurav Bhattacharya will declare that a disaster has occurred and that the

Disaster Recovery Procedure has been activated. Gaurav Bhattacharya also has the discretion to activate the Disaster Recovery Procedure based on other criteria.

4. In the event customer data has been compromised, customers must be notified no later than 72 hours after the incident is reported.
5. Once the Disaster Recovery Procedure has been activated, Gaurav Bhattacharya should notify relevant personnel and executive leadership on the general status of the incident. Notification can be conducted over chat, email, or phone. Gaurav Bhattacharya may also notify the Jeeva AI, Inc. operations team if the disaster involves the Jeeva AI, Inc. premises or is related to Jeeva AI, Inc. employees.
6. If the Disaster Recovery Procedure has not been activated, the Recovery and Reconstitution phases will not be performed. Instead, Gaurav Bhattacharya and necessary team members will perform all appropriate tasks under Jeeva AI, Inc.'s Incident Response Plan.
7. Either Gaurav Bhattacharya or someone they select will document who was contacted and when and will summarize each call.

Recovery Phase

This phase covers the recovery of the application at an alternate site. If the disaster involves both Critical Systems and Non-Critical Systems, the Jeeva AI, Inc. Operations team may prioritize the recovery of Critical Systems and proceed to the Reconstitution Phase for the Critical Systems before Non-Critical Systems have completed the Recovery Phase. This phase consists of the following tasks, some of which can be run in parallel:

1. Assess damage to affected environments, prioritizing critical systems first. Document observations.
2. If possible, back up the affected environments in a forensically sound manner. Do not alter affected systems and applications in any manner.
3. Verify that previous backups of critical databases and systems recovery points are available before moving on to the Reconstitution Phase.

Reconstitution Phase

This phase consists of activities necessary for restoring Jeeva AI, Inc. operations to the original operating state (or permanently move operations to the new site or state, if necessary). If the disaster involves both Critical Systems and Non-Critical Systems, the Jeeva AI, Inc. Operations team may prioritize reconstituting the Critical Systems before beginning reconstitution of the Non-Critical Systems. This phase consists of the following tasks, some of which can be run in parallel:

1. Begin replication of new environment using previously confirmed backups using automated and previously tested scripts.
2. Jeeva AI, Inc. utilizes multiple availability zones; however, if the primary region is unavailable replicated backups should be used to create a production environment in the failover region.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

3. Test new environment using pre-written tests.
4. Test logging, security, and alerting functionality.
5. Verify that systems are appropriately patched and up to date.
6. Deploy new environment to production.

7. Update DNS to new environment.

Forensics Phase

This phase consists of activities related to finding out the cause of the disaster, in cases where it is not immediately apparent. Upon the disaster incident being addressed, with customer data and Jeeva AI, Inc. operating infrastructure recovered and restored, it is appropriate to start the Forensics Phase. This phase consists of the following tasks, some of which can be run in parallel:

1. Ensure all logs from all systems, applications and databases involved in the incident have maintained their integrity in the centralized log repository.
2. If some logs did not reach the central log repository, ensure that missing system, database, and application logs are retrieved. Pay attention to time keeping and clock settings, so logs from different sources can be reconciled.
3. If applicable, transfer data to a log analyzer or test instance.
4. Target network, system, and user action logs for analysis. Analyze all logs manually or with tools, tests, and scripts that have already been previously tested.
5. Document all significant findings in the timeline.

Retrospective Phase

A retrospective of an event such as a disaster recovery incident allows for all parties to understand what happened in a clear and blame-free manner. A retrospective meeting should occur within 72 hours after such an incident has occurred.

1. All relevant parties and system owners should be identified and invited to a retrospective meeting.
2. A draft agenda and disaster timeline should be sent to everyone before the retrospective meeting.
3. Retrospectives are best facilitated with an unbiased third party who was not involved with working the incident. The facilitator should ask questions of meeting participants to illuminate the severity, impact, and any follow-ups.
4. Document the retrospective meeting.
5. Produce an incident report from the retrospective agenda, timeline, and meeting notes.

Reenactment / Test Phase

Unanticipated disasters are unlikely to have documented steps for resolution. Once an unanticipated incident concludes, it should be reenacted to analyze and document how to better respond in the future. If applicable:

1. Run a simulation of the event, as understood by the retrospective meeting notes, timeline, and report. The simulation can be run with people involved or uninvolved with the disaster.
2. While running the simulation, a pre-assigned note taker should write down ideas to prevent

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

and mitigate a similar event.

3. After the reenactment, a new and specific disaster recovery procedure should be created.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Jeeva AI, Inc. management will determine how serious an employee's offense is and take the appropriate action.

Responsibility

The Operations team is responsible for ensuring this policy is followed.

Last updated: *11/20/2024*

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Jeeva AI, Inc. Incident Response Plan

This document offers guidance for employees or incident responders who believe they have discovered or are responding to a security incident.

Escalation

- Email susy@jeeva.ai or message #grafana-alerts on Slack.
- Include as many specifics and details as you can.

Severity

Severity level	Description	Examples	Remediation
Low or Medium Severity	Most issues fall under this category. These do not require someone to be paged or woken up in the middle of the night.	Suspicious emails, outages, strange activity on a laptop	Ping #grafana-alerts
High severity	These are problems where an adversary or active exploitation hasn't been proven yet, and an attack may not have happened, but is likely to happen.	Backdoors, malware, malicious access of business data (e.g. passwords, payment information, vulnerability data, etc.)	@channel to #grafana-alerts
Critical severity	The attackers were successful, and something was lost.		@channel to #grafana-alerts and email susy@jeeva.ai

Internal Issues

When the malicious Actor is an employee, Contractor, vendor, or partner, please contact the CFO directly. Do not discuss the issue with other employees.

Compromised Communications

If there are IT communication risks (i.e. company phones, laptops, email accounts, etc. are compromised) the team will announce an out-of-band communication tool within the office.

Response Steps

For critical issues, the response team will follow an iterative response process designed to investigate,

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

contain the exploitation, remediate the vulnerability, and write postmortem and lessons learned documents.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

1. The CFO should determine if a lawyer should be involved with attorney-client privilege
2. A “War Room” will be designated
3. The following meeting will take place at regular intervals, starting with twice per day, until the incident is resolved

Response Meeting – Agenda

- Update the **Breach Timeline** with all known data related to the incident. The timeline should detail what you’re sure the attacker did at what times.
- Review new **Indicators of Compromise** with the entire group. Indicators of Compromise are anything you know belongs to the attacker: an IP address that sent data, a compromised account, a malicious lie used to spearfish, etc.
- Add new data (knowns and unknowns) to the **Investigative Q&A**, which is a list of questions to which, if you had answers, you’d understand everything the attacker did.
- Update the list of **Emergency Mitigations**: passwords to be reset, laptops to be wiped, IPs to be banned, etc.
- Long Term Mitigations (including Root Cause Analysis): record everything you’ll start doing so this crisis doesn’t happen again.
- Everything Else: communications, legal issues, blog posts, status pages, etc.

Response Team Members

Gautam Bhattacharya, Interim IT Head, 202-714-6689, he/him Susy Pang, CFO, (858) 943-8377, she/her

Required Retrospective

All incidents classified as “High” or above require a retrospective meeting and a “lessons learned” document.

Follow-ups must be completed

All incidents classified as “High” or above require follow-ups to be tasked in a task tracker and completed within a pre-defined time period.

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Jeeva AI, Inc. management will determine how serious an employee’s offense is and take the appropriate action.

Responsibility

The CFO is responsible for ensuring this policy is followed.

Last updated: *11/20/2024*

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Jeeva AI, Inc. Information Security Policy

Jeeva AI, Inc. Security Team

The Jeeva AI, Inc. Security team is comprised of Jeeva AI, Inc.'s following staff:

Susy Pang, Gautam Bhattacharya, Jason Lee

The team is responsible for carrying out all security policies and procedures. The team has a direct line to the CEO and can communicate with the CEO whenever they need to.

Security Officer Role

Susy Pang is the Security Officer. With that title, Susy Pang is responsible for creating and enforcing security policies and procedures; leading the monitoring, vulnerability management, and incident detection and response initiatives; and tracking and reducing risk organization-wide.

People Operations Security

Security Awareness Training

Jeeva AI, Inc. employees and contractors are provided training on the company's security policies and procedures during their first 30 days of employment and annually thereafter. All Jeeva AI, Inc. personnel are then required to acknowledge, electronically, that they have the attended training and understand the security policy.

Security Coding Training

Jeeva AI, Inc. employees and contractors in developer roles are provided with SDLC / Secure Coding training during their first 30 days of employment and annually thereafter. Software developers are trained in secure coding techniques, including how to avoid common coding vulnerabilities. All such personnel are then required to acknowledge, electronically, that they have attended and understand SDLC training and OWASP Top Ten common coding vulnerabilities.

Acceptable Use Policy

Jeeva AI, Inc.'s Acceptable Use Policy covers employee responsibilities and behavior for using Jeeva AI, Inc. systems, including devices, email, internal tools, and social media. Jeeva AI, Inc. employees must acknowledge in writing that they've read and will abide by the Acceptable Use Policy.

All of Jeeva AI, Inc.'s security policies, including the Acceptable Use Policy, are presented to new employees during onboarding, and all employees are required to sign off that they have read all such policies.

Remote Work

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Jeeva AI, Inc. employees who work remotely must follow these rules:

- All company-provided equipment and any equipment used to perform work must remain in the presence of the Jeeva AI, Inc. employee or be securely stored.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

- VPN must be used for all connections with production infrastructure.
- All of Jeeva AI, Inc.'s data encryption, protection standards and settings must be followed for company-provided equipment and any equipment used to perform work.
- The confidentiality, security, and privacy of Jeeva AI, Inc.'s customers must be preserved by ensuring that no unauthorized individuals may view, overhear, or otherwise have access to Jeeva AI, Inc.'s customer data.
  - To enforce, all Jeeva AI, Inc. employees are required to use screen protector's or be conscious of "shoulder surfing" when working in public places like a coffee shop or airport. Jeeva AI, Inc. employees are further required not to teleconference with customers in public areas.
- All remote work must be performed in a manner consistent with Jeeva AI, Inc.'s security policies.

Disciplinary Action

Employees who violate any Information Security policies may face disciplinary consequences in proportion to their violation. Jeeva AI, Inc. management will determine how serious an employee's offense is and take the appropriate action:

- For minor violations, employees may only receive verbal reprimands.
- For more serious violations, employees may face severe disciplinary actions up to and including termination.

Responsibility

The CFO is responsible for ensuring all Information Security policies are followed.

Last updated: *11/20/2024*

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Jeeva AI, Inc. Password Policy

Jeeva AI, Inc.'s Password Policy describes how employees should generate, store, and retrieve their passwords for cloud services they use on behalf of the company or personally.

Password Generation

Jeeva AI, Inc. employees must use complex passwords, where possible, for all of their accounts that have access to Jeeva AI, Inc. data.

"Complex" passwords have at least one uppercase letter, one lowercase letter, one number, and one non-alphanumeric character, and are at least 10 characters long.

All generated passwords for Jeeva AI, Inc. users and system accounts must be unique. Jeeva AI, Inc. employees may not reuse passwords that are or were used elsewhere, e.g. passwords used for personal accounts. A common way attackers obtain access to corporate resources is by using employees' personal passwords that were obtained in breaches of other services.

When creating end user passwords for the first time and/or during a password reset, the CFO must also force the end user to change their password upon logging in for the first time.

Jeeva AI, Inc. employees must always use two-Factor authentication for all accounts that have access to Jeeva AI, Inc. data.

Password Requirements from Services

The services that Jeeva AI, Inc. uses to provide its offering also enforce password rules, which all users (including Jeeva AI, Inc. employees) must follow.

Managing and Storing Passwords

Jeeva AI, Inc. employees are required to use Google Authenticator to manage their passwords and generate sufficiently complex passwords.

All Jeeva AI, Inc. system and user passwords must be encrypted when stored at rest within an application or database. All Jeeva AI, Inc. system and user passwords must be encrypted during transmission.

Under no circumstances should Jeeva AI, Inc. employees share their account passwords with anyone, including other Jeeva AI, Inc. employees.

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Jeeva AI, Inc. management will determine how serious an employee's offense is and take the appropriate action:

- For minor violations, employees may only receive verbal reprimands.
- For more serious violations (e.g. a security incident or breach caused by reuse of personal passwords), employees may face severe disciplinary actions up to and including termination.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Responsibility

The CFO is responsible for ensuring this policy is followed.

Last updated: *11/20/2024*

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Jeeva AI, Inc. Responsible Disclosure Policy

Data security is a top priority for Jeeva AI, Inc., and Jeeva AI, Inc. believes that working with skilled security researchers can identify weaknesses in any technology.

If you believe you've found a security vulnerability in Jeeva AI, Inc.'s service, please notify us; we will work with you to resolve the issue promptly.

Disclosure Policy

- If you believe you've discovered a potential vulnerability, please let us know by emailing us at susy@jeeva.ai. We will acknowledge your email within five business days.
- Provide us with a reasonable amount of time to resolve the issue before disclosing it to the public or a third party. We aim to resolve critical issues within one week of disclosure.
- Make a good faith effort to avoid violating privacy, destroying data, or interrupting or degrading the Jeeva AI, Inc. service. Please only interact with accounts you own or for which you have explicit permission from the account holder.

Exclusions

While researching, we'd like you to refrain from:

- Distributed Denial of Service (DDoS)
- Spamming
- Social engineering or phishing of Jeeva AI, Inc. employees or contractors
- Any attacks against Jeeva AI, Inc.'s physical property or data

centers Thank you for helping to keep Jeeva AI, Inc. and our users

safe!

Changes

We may revise these guidelines from time to time. The most current version of the guidelines will be available at https://involve.ai/disclosure.

Contact

Jeeva AI, Inc. is always open to feedback, questions, and suggestions. If you would like to talk to us, please feel free to email us at susy@jeeva.ai.

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Jeeva AI, Inc. management will determine how serious an employee's offense is and take the appropriate action.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Responsibility

It is the CFO's responsibility to see this policy is enforced. Last updated: *11/23/2024*

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Jeeva AI, Inc. Risk Assessment & Management Program

Jeeva AI, Inc.'s Risk Assessment principles, policies, procedures, and methodology describes what systems Jeeva AI, Inc. has in place to identify new business and technical risks and how often those risks are mitigated.

Principles

Jeeva AI, Inc. is proactive in its approach to risk management, balances the cost of managing risk with anticipated benefits, and undertakes contingency planning in the event that critical risks are realized.

Jeeva AI, Inc. has the primary duty to ensure the Security of critical systems and customer data. A duty to ensure a secure, available infrastructure requires Jeeva AI, Inc. to identify and manage risks.

Jeeva AI, Inc. believes that effective risk management involves:

1. A commitment to the Security of Jeeva AI, Inc. infrastructure and services from senior management.
2. The involvement, cooperation, and insight of all Jeeva AI, Inc. staff.
3. A commitment to initiating risk assessments, starting with discovery and identification of risks.
4. A commitment to the thorough analysis of identified risks.
5. A commitment to a strategy for treatment of identified risks.
6. A commitment to communicate all identified risks to the company.
7. A commitment to encourage the reporting of risks and threat Vectors from all Jeeva AI, Inc.

staff. Jeeva AI, Inc. believes that the following events can trigger a risk assessment to occur:

1. A significant and major change to existing infrastructure, product, or business practices.
2. A significant amount of time (e.g. a year) having passed since the last risk assessment.

Risk assessments can be as high level or detailed to a specific organizational or technical change as Jeeva AI, Inc. stakeholders and technologists see it.

Risk assessments can be conducted by unbiased and qualified parties such as security consultancies or qualified internal staff.

Scope

This Risk Assessment & Management program and policy applies to all systems and data on the Jeeva AI, Inc. network, owned by Jeeva AI, Inc. or its customers, or operated on behalf of the organization.

Risk assessments should evaluate infrastructure such as computer infrastructure containing networks, instances, databases, systems, storage, and services. Jeeva AI, Inc. risk assessments will also include an analysis of business practices, procedures, and physical office spaces as needed.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Risk assessments for vendors are covered under Jeeva AI, Inc.'s Vendor Management Program, which includes a thorough risk assessment targeted at a vendor's security, business practices, legal commitments, and insurance postures.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Definitions

Risk

Risk is the probability that a harmful consequence may result when exposed to a hazard. Risk is characterized and rated by considering two Factors:

1. Probability or likelihood (L) of occurrence; and
2. Consequence (C) of occurrence.

This is expressed as R (risk) = L (likelihood) x C (consequence).

Threat

A potential incident or activity which may be deliberate, accidental, or caused by nature which may cause physical harm to a person or financial harm to an organization.

Likelihood

Likelihood is a qualitative description of probability or frequency. The likelihood of occurrence is a weighted risk Factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities). The likelihood risk Factor combines an estimate of the likelihood that the threat event will be initiated with an estimate of the likelihood of impact (i.e., the likelihood that the threat event results in adverse impacts).

Consequence

Consequence is the outcome of an event and is a loss, disadvantage, or gain. There are a range of possible outcomes associated with an event. Consequence and impact are used interchangeably. The level of impact from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Risk Assessment

A risk assessment is the process of evaluating and comparing a level of risk against predetermined acceptable levels of risk. It is an examination of all possible risks along with implemented and non-implemented solutions to reduce, eliminate, or manage the risks.

Risk Management

Risk management is the application of a management program that addresses organizational and technical risk. This management program includes identification, analysis, treatment, and monitoring.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Risk Owner

A risk owner is the person responsible for managing an individual risk. The risk owner is typically the person directly responsible for the strategy, activity, or function that relates to that risk.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Risk Assessment & Management Policy

This risk assessment policy specifies how and when risk assessments will be done and who will be responsible for conducting risk assessments and implementing solutions to address any risk assessment findings.

It is the responsibility of all Jeeva AI, Inc. staff to identify, analyze, evaluate, monitor, and communicate risks associated with any activity, technology, function, or process within their relevant scope of responsibility and authority. Staff identifying potential risks or vulnerabilities are to report them to internal staff and/or external third parties.

Overall, the execution, development, and implementation of risk assessments and remediation programs is the joint responsibility of Jeeva AI, Inc.'s CFO and the department or individuals responsible for the surface area being assessed. All staff are expected to cooperate fully with any risk assessment being conducted on systems and procedures for which they are responsible. Staff are further expected to work with the risk assessment project lead in the development of a remediation plan for each risk assessment performed.

- Jeeva AI, Inc. performs at least one risk assessment, at a minimum, every six months using qualified internal staff and/or external third parties who have experience performing risk assessments.
- A risk assessment should be done or reviewed on critical systems and applications no less than every two years.
- Risk assessments may be used to assess all risks to the organization.
- All staff involved with a risk assessment must fully cooperate with the risk assessment project lead in conducting the assessment and developing a remediation strategy.
- Any staff members or external consultants who perform any Jeeva AI, Inc. risk assessments are required to be familiar with computer technology and computer security in particular. The risk assessment project leader should be the security officer, or a staff member designated by the security officer to conduct the risk assessment.
- Risk assessment deliverables include a risk assessment report with a risk reduction action plan to manage or mitigate any unacceptable risks. The action plan may be included with the risk assessment report, or separately. The action plan will be a plan for implementing additional controls and solutions to mitigate or manage the risk. The action plan may define participants and actions to be taken during the implementation of the action plan.
- The risk assessment process and methodology will be updated as required due to results of audits and incidents.
- All identified vulnerabilities will be assessed for impact and criticality. Vulnerabilities must be remediated as soon as possible as mandated by the Jeeva AI, Inc. Vulnerability and Patch Management Program.

Risk Assessment Process

Jeeva AI, Inc. risk assessment methodology is based off *NIST Special Publication 800-30 Revision 1 – Guide for Conducting Risk Assessments*.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

- Management defines the scope of risk assessment and creates the risk assessment team with a point person to guide the process (risk assessment project lead).

- If risk assessment procedures are not denied, the team should define them. The proper time and method of communicating the selected risk treatment options to the affected IT and business management should be included.
- Evaluate the system – Determine if the system is critical to the organization's business processes and determine the data classification and security needs of the data on the system according to the Jeeva AI, Inc. Data Classification Policy, considering Security needs.
- List the threats - List possible threat sources such as an exploitation of a vulnerability.
- Identify vulnerabilities.
- Evaluate potential security controls already in place to assess if they adequately address the risk.
- Identify probability of exploitation. Additional security controls may need to be in place before the probability of exploitation is lowered.
- Quantify damage (impact) – Categorize the damage and possibly place a dollar amount on the damage where possible. This will help when looking at cost of controls to reduce the risk.
- Determine risk level - Use likelihood times impact to quantify the amount of risk.
- Evaluate and recommend controls to reduce or eliminate risk - Identify existing controls and those that may further reduce probabilities or mitigate specific vulnerabilities. List specific threats and vulnerabilities for the system to help identify mitigating controls.
- Create the risk assessment report.
- Communicate the selected risk treatment options to the affected IT and business management and staff.
- Take recommended risk mitigation actions. Record such actions as changes per the Jeeva AI, Inc. Change Management program.
- Monitor the effectiveness of the risk mitigation actions and document the results.

Risk Mitigation Standards

Acceptable Risks

When the probability of threat materialization times maximum damage amount is less than $1000 annually, the risk is acceptable. For higher amounts, on a yearly basis, acceptance of the risk will depend on the cost of implementing measures to reduce the risk. If the risk cannot be reduced and the amount per year is greater than $50,000, the risk should be transferred by purchasing insurance.

Risk Mitigation

Options for mitigating risk shall include the following possibilities:

- Reducing the chance of an occurrence of an event
- Reducing the damage due to occurrence

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

- Avoiding the risk
- Transferring the risk by taking an action such as purchasing insurance

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Some guidelines and standards applicable to Jeeva AI, Inc.:

- Costs of implementing each control are considered and compared to the benefits, pecuniary and non-pecuniary, of implementing each control.
- Cost and benefit analysis is done to evaluate proposed controls versus risks. When the controls are evaluated, the benefits, costs, and cost savings of applying the controls both individually and in combination should be determined. Performance measures for determining the effectiveness of the new controls are created.
- Risks shall be ranked, and controls are selected, and a plan created to implement the controls. Responsibilities for implementing the controls are determined and communicated. Budgeting and schedules are set and the expected outcomes from mitigating the risks with the controls are documented. Residual risk after full implementation is considered.
- Decisions regarding residual risk are made. Specifically, whether to accept the risk, transfer the risk, or take other action, including adding additional controls.
- Safeguard options for addressing high risk scenarios must be considered and utilized appropriately while the extent of risk reduction and benefits are considered. Cost and benefit analysis is done to evaluate safeguard options.
- If the cost of safeguard options or recommended risk controls is greater than the available budget, the options and controls are prioritized to reduce as much risk as possible within the budget.
- When the risk assessment report is completed, results shall be communicated to the affected IT and business management and staff.

Non-Compliance

Since risk assessments are an important part of protecting data and systems for Jeeva AI, Inc., employees that purposely violate this policy may be subject to disciplinary action up to and including denial of access, legal penalties, and/or dismissal. Any employee aware of any violation of this policy is required to report it to their supervisor or other authorized representative.

Responsibility

The CFO is responsible for communicating detected risks and remediation steps needed to the appropriate staff for resolution. Those staff members are then responsible for resolving detected risks in a timely manner, guided by the severity of the detected risk.

Last updated: *11/23/2024*

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Jeeva AI, Inc. System Access & Authorization Control Policy

Each Jeeva AI, Inc. employee, Contractor, and associate has limited access to Jeeva AI, Inc. systems and applications. Access is always provisioned on a minimum-necessary (least-privilege) basis.

Employee Access to Jeeva AI, Inc. Systems

Access to Jeeva AI, Inc. systems and third-party accounts owned by Jeeva AI, Inc. will only be granted on a need-to-use basis, as defined by the responsibilities of the position held and the duties of that position.

Access control and management is divided into multiple phases of an account lifecycle: creation, privilege management, authorization, password management, audit, and revocation.

Authorization: Role Based Access Control

- In most cases, Jeeva AI, Inc. employees are granted access to Jeeva AI, Inc. systems according to their role and/or team.
- The executive team and team managers are jointly responsible for maintaining a list of roles and associated access scope for team members.
- If a Jeeva AI, Inc. employee requires access outside of the standard for their role or team, either they or their managers may initiate an access request, following the policy outlined in "access requests" below.

Creation: Access Requests

- Access requests for Jeeva AI, Inc. employees are made by employees and their managers.
- Access requests should be made to the Jeeva AI, Inc. employee or employees who manage the relevant resource(s).
- Those employees will not grant access unless they are satisfied the additional access is necessary for the grantee to complete a necessary business task.
- When granting access, employees will ensure grants are scoped to the minimum breadth and duration to complete the relevant business task. Root access will not be granted unless absolutely necessary to perform the job function.

In addition, the employee(s) must accept the company's Acceptable Use Policy before access will be granted.

Privilege Management

- Jeeva AI, Inc.'s Operations team will determine and maintain appropriate assignment of privilege within Jeeva AI, Inc.'s production, development and test applications and environments.
- Jeeva AI, Inc.'s Operations team will determine and maintain appropriate assignment of

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

privilege within Jeeva AI, Inc.'s databases.

- Jeeva AI, Inc.'s Operations team will determine and maintain appropriate assignment within supporting infrastructure.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Account Audit

- The responsible team will conduct quarterly audits of accounts, privileges, and password management, and is required to document findings and changes in Zendesk.

Revocation: Role Changes & Termination

- Managers must notify Jeeva AI, Inc.'s Operations team if an employee has been terminated or changes role.
- In the case of termination, the former employee's access is required to be revoked within reasonable timelines as defined by company procedural commitments in Vanta.
- In the case of a role change, the employee's access should be revised within reasonable timelines as defined by company procedural commitments in Vanta.
- In some cases, access will be revoked as a disciplinary measure for policy violation.

Employee Authentication to Jeeva AI, Inc. Systems

Authentication

Each Jeeva AI, Inc. employee has a unique user ID and password that identifies them as the user of a Jeeva AI, Inc. IT asset or application. All assets, applications and vetted third party platforms may be required to have two-Factor authentication configured.

Password, Key, and Certificate Management

As specified in the Acceptable Use Policy and Password Policy, Jeeva AI, Inc. employees must use complex passwords and multi-Factor authentication for all Jeeva AI, Inc.-related accounts. User passwords must conform with the restrictions set forward in the Jeeva AI, Inc. Password Policy. Please see Acceptable Use Policy and Password Policy for further details and guidance.

Jeeva AI, Inc.'s IT team is responsible for issuing and revoking SSH keys in all environments.

Jeeva AI, Inc.'s Engineering team is responsible for issuing, renewing, and revoking public web and internal SSL certificates.

Customer Data

Employees that require access to customer data must have an individual account. This account, as well as actions performed with it, will be subject to additional monitoring at the discretion of the management team and subject to applicable regulations and third-party agreements.

At a minimum, employees with access to customer data can expect that their actions in customer-data systems (e.g. an internal admin tool) will be logged, with the logs stored centrally for at least 12 months.

Guest Access to Jeeva AI, Inc. Systems

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Occasionally, guests will have a legitimate business need for access to the corporate network. When such need is demonstrated, temporary guest access to company systems is permitted. This access,

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

however, must be severely restricted to only those resources that the guest needs at that time, and disabled when the guest's work is completed.

Guest Wireless Use

Jeeva AI, Inc.'s production systems are not accessible directly over wireless channels, and connecting to the company guest wireless network should grant no extra privileges or access to company systems.

All employees have access to the networking equipment that is used by the Jeeva AI, Inc. office network. It is each employee's responsibility to ensure that the equipment is not tampered with.

Wireless passwords are not reset on a regular cadence.

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Jeeva AI, Inc. management will determine how serious an employee's offense is and take the appropriate action:

- For minor violations, employees may only receive verbal reprimands.
- For more serious violations that lead to security incidents, employees may face severe disciplinary actions up to and including termination.
- Jeeva AI, Inc. employees will not be disciplined for surfacing deficiencies or misconfigurations that contradict this policy.

Responsibility

Each Jeeva AI, Inc. employee is responsible for surfacing technical misconfigurations and deficiencies to the Operations team for immediate resolution.

The Operations team is responsible for ensuring this policy is followed.

Last updated: *11/23/2024*

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Jeeva AI, Inc. Vendor Management Policy

Jeeva AI, Inc. relies on vendors to perform a range of services, some of which are critical for operations.

Jeeva AI, Inc. aims to manage its relationship with vendors and minimize the risk associated with engaging third parties to perform services. This policy provides a framework for managing the lifecycle of vendor relationships.

Vendor Risk Assessment

For each potential vendor, conduct an initial risk analysis, assigning the vendor a "low," "medium," or "high" rating based on the highest risk level attributable to the contract.

	Low	Medium	High
Business impact	Nominal impact could get along without it. Does not connect to any piece of Jeeva AI, Inc. infrastructure.	Significant but non-critical business im-pact	Mission critical
Customer facing?	No	Indirect	Direct
Access to customer data	No access	Access to often public but personally-identifiable information (e.g. email ad- dresses)	Access to non-public personally-identifiable information (e.g. email content)

The rating indicates the level of due diligence Jeeva AI, Inc. requires for each vendor:

- **Low-risk** vendors typically require little analysis
- **Medium-risk** vendors should be evaluated to determine the appropriate level of due diligence required
- **High-risk** vendors require extensive review

Vendor Assessment Process

Risk assessments should be conducted before doing business with a new vendor and revisited when the relationship with the vendor changes significantly, including contract renewals. All vendors are required to be reassessed annually.

An assessment of the proposed vendor is initiated when a Vendor Sponsor (anyone at Jeeva AI, Inc. looking to do business with a vendor) submits a review request to the Operations team.

The Vendor Sponsor may wish to sign a mutual Non-Disclosure Agreement (mNDA) with the proposed vendor. The proposed vendor and the Vendor Sponsor should sign the mNDA before the Vendor Sponsor:

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

- discloses Jeeva AI, Inc. information to determine company/vendor fit
- accepts a completed Vendor Assessment Questionnaire (VAQ), which contains the vendor's operating information.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

The Vendor Sponsor should then submit the mNDA (if applicable), VAQ, and other relevant collateral to the Operations team for review. The Operations team will complete the review in a timely manner and communicate next steps to the Vendor Sponsor. All reviews should be documented in meeting notes, for security, legal, and audit. When the Operations team approves the vendor, the Jeeva AI, Inc. Vendor Sponsor may move forward with contract negotiations. The Operations team must provide documented approvals to the Vendor Sponsor. The Finance team may set the vendor up for payment. The Finance team will be responsible for ensuring the Operations team documented their signoff.

Vendor Assessment Due Diligence

Due diligence entails making a reasonable inquiry into a vendor's ability to meet the requirements for the proposed service. Jeeva AI, Inc. first sends the proposed vendor a Vendor Assessment Questionnaire. Once the VAQ is completed, the Operations team reviews the responses and either clears the vendor, rejects the vendor, or requests further information.

A due diligence review might include further discussions regarding the following topics:

- **Regulatory**: Can the vendor create regulatory risk for Jeeva AI, Inc.?
- **Reputation**: How might the vendor impact Jeeva AI, Inc.'s reputation?
- **Financial**: Can the vendor impact Jeeva AI, Inc. or its customers financially?
- **Access to customer data**: To what extent will the vendor handle sensitive Jeeva AI, Inc. data?
- **Operational effectiveness**: How might Jeeva AI, Inc. be affected if the vendor experienced downtime? If the vendor ceased operations suddenly? Are there other potential vendors that Jeeva AI, Inc. could work with in such cases?
- **Compensating controls:** Does the vendor offer multi-Factor authentication on its service? Can that be enforced such that all Jeeva AI, Inc. users must turn on MFA to use the service?

Vendor Compliance Considerations

If the vendor has a SOC 2, ISO27001/2, or other relevant collateral, it should be collected, reviewed by the Operations team, and documented in Jeeva AI, Inc. records.

Managing Vendors

Vendor Supervision

Each vendor will be assigned a Vendor Sponsor who will act as a liaison between the vendor and Jeeva AI, Inc.

Vendor List

The Operations team maintains a complete list of all vendors, associated risk rankings, the Vendor Relationship Manager, and the date of the most recent evaluation.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Vendor Configuration

Multi-Factor authentication should be enabled on all accounts for all vendors.

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Jeeva AI, Inc. management will determine how serious an employee's offense is and take the appropriate action:

- For minor violations, employees may only receive verbal reprimands.
- For more serious violations (e.g. onboarding a vendor without appropriate review and due diligence), employees may face severe disciplinary actions up to and including termination.

Responsibility

The Jeeva AI, Inc. Vendor Sponsor is responsible for ensuring prospective vendors enter the vendor review process.

The Operations team is responsible for ensuring this policy is followed.

Last updated: *11/23/2024*

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Jeeva AI, Inc. Vulnerability Management & Patch Program

Jeeva AI, Inc.'s Vulnerability Management policies and procedures describe what systems are in place to monitor for new vulnerabilities, how often vulnerabilities are addressed, and the way in which those vulnerabilities are addressed.

On average, 20-30 new vulnerabilities are released into the wild every day. Jeeva AI, Inc.'s internal vulnerability monitoring and external vulnerability scanning are in place to keep up with new threats while validating security controls put in place so that Jeeva AI, Inc.'s security posture is maintained.

Vulnerability Management & Patch Policy

- Jeeva AI, Inc. performs internal vulnerability scanning and package monitoring on a constant basis using:
  - GitHub, Vanta, Sonar Cloud
- Jeeva AI, Inc. performs external vulnerability scanning Every build using Sonar Cloud. The following are the focus of external vulnerability scanning: external web apps, company APIs.
- The Tech lead(s) is responsible for communicating detected vulnerabilities and package updates needed to the appropriate engineering staff for resolution. Engineering staff responsible for various infrastructure components are responsible for resolving detected vulnerabilities in a timely manner as defined by Jeeva AI, Inc.'s timing standards, as defined below.

Severity & Timing

Jeeva AI, Inc. defines the severity of an issue via industry-recognized Common Vulnerability Scoring System (CVSS) scores, which all modern scanning and continuous monitoring systems utilize. The CVSS provides a way to capture the characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

All vulnerabilities will be addressed within reasonable timelines as defined by company procedural commitments.

Low Severity - 0.1 - 3.9

Low severity vulnerabilities are likely to have very little impact on the business, perhaps because they require local system access.

Medium Severity – 4.0 – 6.9

Medium severity vulnerabilities usually require the same local network or user privileges to be exploited.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

High Severity - 7.0 - 8.9

High severity vulnerabilities are typically difficult to exploit but could result in escalated privileges, significant data loss, and/or downtime.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Critical Severity – 9.0 – 10.0

Critical severity vulnerabilities likely lead to root level compromise of servers, applications, and other infrastructure components. If a critical vulnerability cannot be addressed within timelines as defined, an incident response ticket will be opened, documenting what interim remediation has been made.

Vulnerability & Patch Management Process

1. A new vulnerability or a new patch is detected from the various monitoring and scanning Jeeva AI, Inc. has in place.
2. The Tech lead(s) enters vulnerability details or patch instructions into Jeeva AI, Inc.'s change management system, which is GitHub Projects , and assigns the ticket to the appropriate team member to address.
3. The ticket assignee follows the change management process to implement the necessary change to apply the patch or address the new vulnerability.
4. The ticket is updated with results from the applied change, detailing any exceptions into the Jeeva AI, Inc. risk register.
5. The Tech lead(s) checks the source from which the vulnerability originated to ensure that the change performed has addressed the vulnerability detected. The ticket is updated with the results and closed out.

Exceptions

Any exception to the policy must be approved by the Tech lead(s) in advance and placed on the risk register for monitoring and periodic review.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including employment termination.

Responsibility

It is the CFO's responsibility to ensure this policy is followed.

Reviewing vulnerability scans and continuous monitoring findings, and dividing up resolution tasks, are the responsibility of the Tech lead(s).

All engineers and developers are responsible for investigating and resolving vulnerabilities assigned to them via patching and configuration changes, as they are assigned.

Last updated: *11/23/2024*

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Formal AI / ML Governance Policy

Jeeva AI, Inc. has established a robust Artificial Intelligence and Machine Learning (AI/ML) governance policy, structured to ensure ethical, transparent, and compliant use of AI systems throughout their entire lifecycle. This policy is aligned with international standards such as ISO/IEC 42001:2023 and incorporates best practices for risk management, accountability, and continuous improvement

Model Lifecycle Management

The governance framework covers all stages of the AI/ML model lifecycle, including:

- **Inception:** Identification of business needs, stakeholder alignment, and feasibility assessment.
- **Design and Development:** Definition of system architecture, data flows, and model training procedures, with a focus on explainability and traceability.
- **Verification and Validation:** Rigorous testing to confirm that models meet predefined requirements and perform as intended in various scenarios.
- **Deployment:** Controlled release of models into operational environments, with clear documentation and risk controls.
- **Operation and Monitoring:** Ongoing performance monitoring, logging, and outcome assessment to detect issues such as data drift or model degradation.
- **Re-evaluation:** Periodic reassessment to ensure continued fitness for purpose, especially as conditions or regulatory requirements evolve.
- **Retirement/Decommissioning:** Structured decommissioning of obsolete models, including archiving, documentation of rationale, and communication with stakeholders

Bias Testing and Fairness Audits

This policy mandates systematic bias detection and mitigation at multiple points in the model lifecycle:

- **Data Audits:** Regular reviews to identify representation gaps and potential sources of bias in training data.
- **Model Audits:** Examination of model structure and feature importance to uncover hidden or proxy biases.
- **Fairness Metrics:** Use of statistical tests (e.g., confusion matrices, ROC curves) to compare outcomes across demographic groups and ensure equitable treatment.
- **Real-World Impact Assessment:** Evaluation of model behavior in practical use cases, with a focus on minimizing disparate impacts on marginalized populations.
- **Documentation:** Detailed reporting of bias audit findings, mitigation actions, and ongoing monitoring results

Human-in-the-Loop (HITL) Mechanisms

Human oversight is integrated at critical decision points to ensure that AI systems remain aligned with organizational values and ethical standards:

- **Annotation and Training:** Human experts are involved in labeling data and refining model parameters.
- **Decision Oversight:** For high-stakes or sensitive applications, human review is required before final decisions are enacted.
- **Continuous Feedback:** Mechanisms are in place for users and stakeholders to provide feedback, enabling iterative improvement and accountability.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Decommissioning and Archival Protocols

This policy specifies clear procedures for model retirement:

- **Obsolescence Evaluation:** Models are regularly assessed against performance benchmarks to determine continued relevance.
- **Risk Assessment:** Potential risks of retaining outdated models are evaluated, particularly in regulated sectors.
- **Systematic Withdrawal:** Decommissioned models are archived, with all associated data and documentation preserved for compliance and future reference.
- **Stakeholder Communication:** All relevant parties are notified of decommissioning timelines and rationales to ensure transparency and operational continuity.
- **Ethical Considerations:** The impact of decommissioning on affected individuals and communities is carefully considered, especially regarding the mitigation of any residual biases or harms.

Documentation and Periodic Review

All governance activities, including model inventory, compliance audits, bias testing, and decommissioning decisions, are meticulously documented. The policy is subject to regular review by a cross-functional AI oversight committee, with updates made as necessary to reflect evolving regulations, organizational priorities, and technological advancements.

This comprehensive approach ensures that AI/ML systems are managed responsibly, remain compliant with legal and ethical standards, and continue to deliver value while minimizing risks throughout their lifecycle.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

AI-Specific Employee Training Curriculum

An annual AI-specific employee training curriculum is in place, consisting of a structured syllabus delivered through interactive presentations and training modules. The curriculum covers foundational AI concepts, ethical considerations, regulatory compliance, and practical applications, with mandatory completion tracked and enforced on an annual basis. Employees are required to attend refresher sessions each year to maintain awareness of evolving best practices and regulatory requirements.

Curriculum Structure

- The training program is delivered through a combination of interactive presentations, instructor-led workshops, and self-paced online modules.
- Employees are provided with a detailed syllabus at the start of each training cycle, outlining session topics, learning objectives, and assessment criteria.
- The curriculum is structured to accommodate varying levels of prior AI knowledge, ensuring accessibility for both technical and non-technical staff.

Core Content Areas

- **Foundational AI Concepts:** Introduction to machine learning, deep learning, natural language processing, and other key AI methodologies.
- **Ethical Considerations:** Exploration of ethical principles such as fairness, transparency, accountability, and the mitigation of bias in AI systems.
- **Regulatory Compliance:** Overview of applicable laws and standards, including GDPR, cross-border data transfer mechanisms, and sector-specific regulations.
- **Practical Applications:** Case studies and scenario-based exercises illustrating the responsible use of AI in the organization's operational context.
- **Risk Management:** Identification and management of risks associated with AI deployment, including data privacy, security, and unintended consequences.

Assessment and Certification

- Completion of the training is verified through quizzes, practical assignments, and scenario-based evaluations.
- Employees must achieve a passing score on all assessments to be certified as compliant with the organization's AI training requirements.
- Training records are maintained by the Human Resources department, with completion status tracked and reported to management.

Annual Refresher Requirement

- All employees are required to participate in annual refresher sessions to stay informed of evolving best practices, technological advancements, and regulatory updates.
- Refresher content is updated each year based on changes in the legal landscape, organizational policies, and emerging risks.
- Non-compliance with the annual training requirement may result in restricted access to AI-related systems or disciplinary action.

Continuous Improvement

- Feedback from participants is solicited after each training cycle to inform ongoing improvements to the curriculum.

- The training program is reviewed annually by the AI Governance Committee to ensure alignment with organizational objectives and external standard

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

UK/EEA Cross-Border Transfer Procedure Policy

Jeeva AI, Inc. has a cross-border data transfer procedure, that is designed to ensure that all personal data transfers from the United Kingdom (UK) and European Economic Area (EEA) are conducted in strict compliance with applicable data protection laws, including the UK GDPR and EU GDPR. This procedure is regularly updated to reflect changes in legal requirements and regulatory guidance.

Adequacy Decisions

- Transfers of personal data from the EEA to the UK currently benefit from an adequacy decision by the European Commission, which confirms that the UK provides an essentially equivalent level of data protection to the EU. This adequacy decision is set to expire on June 27, 2025, but a proposed extension would allow free flows of personal data to continue until December 27, 2025, pending review of the UK's data protection framework.
- As long as the adequacy decision remains in effect, personal data can flow freely between the EEA and the UK without requiring additional safeguards.

Standard Contractual Clauses (SCCs) and International Data Transfer Agreement (IDTA)

- In the absence of an adequacy decision, or for transfers to countries not covered by such a decision, the organization utilizes Standard Contractual Clauses (SCCs) as approved by the European Commission for EEA transfers, and the International Data Transfer Agreement (IDTA) or the UK Addendum to the SCCs for UK transfers.
- SCCs are legally binding contracts that impose data protection obligations on both the data exporter and importer, ensuring that personal data remains protected to EU standards during and after transfer.
- The IDTA is used for transfers from the UK to countries outside the EEA, and the UK Addendum allows the use of EU SCCs in a UK context, ensuring compliance with UK GDPR.

Transfer Risk Assessments

- Whenever SCCs, the IDTA, or the UK Addendum are used, the organization conducts a written risk assessment—known as a Transfer Impact Assessment (TIA) in the EU or a Transfer Risk Assessment (TRA) in the UK—to evaluate whether the destination country provides adequate protection for personal data.
- This assessment considers the legal environment of the recipient country, the nature of the data, and the likelihood of unauthorized access by public authorities.

Contractual Safeguards and Supplementary Measures

- Where necessary, supplementary technical and organizational measures (such as encryption, pseudonymization, or strict access controls) are implemented to mitigate identified risks and ensure the ongoing protection of personal data during cross-border transfers.
- All contractual arrangements are reviewed and updated as required to reflect changes in law, regulatory guidance, or organizational risk assessments.

Documentation and Transparency

- All cross-border transfers are documented, including the legal basis for transfer, the results of risk assessments, and the safeguards applied.
- Jeeva AI, Inc. privacy notice and internal records are updated to reflect the nature and scope of international data transfers, ensuring transparency for data subjects and regulatory authorities.

Ongoing Monitoring and Compliance

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

- Jeeva AI, Inc. continuously monitors developments in UK and EU data protection law, including the status of adequacy decisions and legislative reforms, to ensure that its cross-border transfer procedures remain compliant.
- In the event of changes to adequacy status or regulatory requirements, the organization is prepared to promptly implement alternative transfer mechanisms to maintain lawful data flows and minimize business disruption.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

HR Procedure Policy

Jeeva AI, Inc. human resources (HR) procedures are designed to support the entire employee lifecycle, ensuring that all processes are conducted in a structured, consistent, and legally compliant manner. These procedures are intended to promote fairness, transparency, and accountability at every stage of employment.

Recruitment and Hiring

- The recruitment process begins with the creation of a detailed job description and candidate profile, followed by the posting of vacancies through approved channels.
- All applicants undergo a standardized screening process, including resume reviews, structured interviews, and, where applicable, skills assessments.
- Selection decisions are made based on objective criteria aligned with the requirements of the role, with a commitment to equal opportunity and non-discrimination.
- Offers of employment are extended in writing, outlining terms and conditions of employment, and are contingent upon successful completion of background checks.

Background Checks

- Comprehensive background checks are conducted for all new hires, including verification of identity, employment history, educational qualifications, and, where relevant, professional licenses or certifications.
- Additional checks, such as criminal record screening or credit checks, may be performed for roles with heightened security or financial responsibilities, in accordance with applicable laws and organizational policies.
- All background check procedures are carried out with respect for privacy and data protection laws, and candidates are informed of the scope and purpose of these checks before they are initiated.

Onboarding

- New employees participate in a structured onboarding program, which includes orientation sessions, training on company policies and procedures, and completion of required documentation.
- Onboarding is designed to ensure that employees understand their roles, responsibilities, and the organization's expectations from the outset.

Performance Management and Disciplinary Procedures

- The organization maintains a clear performance management framework, including regular feedback, performance appraisals, and opportunities for professional development.
- Disciplinary procedures are defined in a written policy and are initiated in cases of misconduct, performance issues, or violations of company policy.
- The disciplinary process involves a fair and impartial investigation, clear communication of concerns, and an opportunity for the employee to respond.
- Disciplinary actions may include verbal or written warnings, suspension, or other corrective measures, escalating to termination if warranted.

Termination Procedures

- Termination of employment may occur due to resignation, redundancy, retirement, or dismissal for cause.
- All terminations are managed in accordance with applicable employment laws and contractual obligations, ensuring proper notice periods, final compensation, and return of company property.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

- Exit interviews are conducted to gather feedback and ensure a smooth transition for both the departing employee and the organization.

Documentation and Compliance

- Each stage of the HR process is thoroughly documented, with records maintained securely in compliance with data protection regulations.
- Procedures are regularly reviewed and updated to reflect changes in legal requirements, industry best practices, and organizational priorities.
- HR staff receive ongoing training to ensure consistent application of procedures and adherence to ethical standards.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Anti-Bribery and Anti-Corruption Policy

Jeeva AI, Inc. maintains a comprehensive Anti-Bribery and Anti-Corruption (ABAC) policy, which establishes a zero-tolerance stance toward bribery, corruption, and all forms of unethical conduct in business operations. This policy applies to all employees, officers, directors, contractors, and third-party representatives acting on behalf of the organization.

Policy Scope and Prohibitions

- The ABAC policy strictly prohibits the offering, giving, solicitation, or acceptance of any bribe—whether cash, gifts, hospitality, or other advantages—with the intent to improperly influence business decisions, secure an improper advantage, or obtain or retain business.
- Corrupt practices, including facilitation payments, kickbacks, or any other form of illicit inducement or reward, are expressly forbidden.
- The policy covers all business dealings and transactions in every country where the organization operates, including interactions with government officials, commercial partners, and private individuals.

Employee Responsibilities and Training

- All employees are required to read, acknowledge, and adhere to the ABAC policy as a condition of employment.
- Employees must complete mandatory training on anti-bribery and anti-corruption principles during onboarding and participate in annual refresher courses to maintain awareness of evolving risks and regulatory requirements.
- Employees are obligated to promptly report any suspected or actual violations of the policy through designated internal reporting channels, with assurances of confidentiality and protection against retaliation.

Due Diligence and Third-Party Management

- The organization conducts appropriate due diligence on third parties, including vendors, consultants, and agents, to assess and mitigate bribery and corruption risks prior to engagement.
- All third-party agreements include contractual clauses requiring compliance with anti-bribery and anti-corruption standards.

Monitoring, Enforcement, and Disciplinary Action

- Compliance with the ABAC policy is monitored through regular audits, risk assessments, and internal controls.
- Any breach of the policy is subject to disciplinary action, up to and including termination of employment or contract, and may result in legal proceedings where applicable.

Policy Review Cadence

- The ABAC policy is reviewed annually each June to ensure its continued relevance, effectiveness, and alignment with current laws and best practices.
- The most recent approval of the policy was on June 15, 2024, and the next scheduled review will occur in June 2025.
- Updates or revisions to the policy are communicated promptly to all employees and relevant stakeholders.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Physical Security Policy

Version: 2.3
Effective Date: Oct 01, 2024
Policy Owner: Head of IT
Approval: Jeeva AI Management Team

Purpose of this Policy

This policy establishes the physical security requirements and procedures for Jeeva AI to protect its people, facilities, equipment, and information assets from physical threats such as unauthorized access, theft, vandalism, and natural disasters. The goal is to ensure a secure environment that supports the safe development and operation of Jeeva AI staff and the security of Jeeva AI technology and data.

Scope

This policy applies to all Jeeva AI employees, contractors, visitors, and third parties who access Jeeva AI premises, data centers, or any location where company assets are stored or processed. It covers all physical locations operated or leased by Jeeva AI, including offices, server rooms, and co-working spaces.

Policy Statement

Jeeva AI is committed to safeguarding its physical and informational assets through layered security controls, ongoing risk assessment, and continuous improvement. All personnel must adhere to the controls and procedures outlined in this policy. The Head of IT is responsible for maintaining, reviewing, and updating this policy annually or as needed.

Roles and Responsibilities

- *Head of IT:* Policy owner; responsible for implementation, maintenance, review, and communication of this policy.
- *All Employees/Contractors:* Must comply with physical security procedures and report incidents or suspicious activity.
- *Facilities Management:* Implements and maintains physical security infrastructure (e.g., access controls, surveillance).
- *Security Personnel:* Monitors premises, responds to incidents, and enforces access controls.

Physical Security Controls

A. Deter

- Perimeter fencing, clear signage, and visible security cameras at all entry points.
- Security awareness training for all staff to recognize and report suspicious behavior.

B. Detect

- 24/7 CCTV surveillance in critical areas (entrances, server rooms, workspaces).
- Intrusion detection systems and motion sensors in sensitive zones.
- Visitor logs and badge systems to track all non-employee access.

C. Delay

- Electronic access control systems (keycards, biometrics) for all main entrances and restricted areas (e.g., server rooms).
- Physical barriers (locked doors, security turnstiles) to delay unauthorized entry.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

- Segregation of sensitive areas with tiered access permissions.

D. Respond

- Incident response protocols, including immediate notification of the Head of IT and law enforcement if necessary.
- Emergency communication systems and evacuation procedures.
- Regular drills and tabletop exercises for security incidents.

Asset Protection

- All company equipment must be recorded in an asset management system.
- Laptops and mobile devices must be encrypted; sensitive documents stored in locked cabinets.
- Regular audits of physical assets and access logs.

Access Control Procedures

- Access to facilities is granted based on job function and reviewed quarterly.
- All visitors must be escorted and wear visitor badges at all times.
- Terminated employees or contractors have access revoked immediately.

Monitoring and Review

- The Head of IT will conduct annual reviews and risk assessments to ensure policy effectiveness and compliance.
- Policy updates will be communicated to all staff, with mandatory training sessions following significant changes.
- Regular testing of security systems and periodic third-party audits.

Policy Communication

- This policy is distributed to all employees and contractors upon onboarding and is available on the company intranet.
- Updates and reminders are communicated via email and during quarterly all-hands meetings.

Enforcement

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract.

Policy Review and Maintenance

The Head of IT is responsible for reviewing this policy at least annually or following any significant security incident, organizational change, or regulatory update. All updates must be approved by management and communicated to all relevant parties.

Approved by: Jeeva AI Management Team
Policy Owner: Head of IT
Next Review Date: Sep 30, 2025

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

Third Party Risk Monitoring Policy

Version: 1.1
Effective Date: Nov 1, 2024
Policy Owner: Head of IT
Approval: Jeeva AI Management Team

Purpose

This policy establishes the framework for identifying, assessing, selecting, overseeing, and continuously monitoring third parties—including subcontractors, service providers, dependent service providers, and sub-processors—engaged by Jeeva AI. The objective is to protect Jeeva AI's operations, data, and reputation by managing risks associated with third-party relationships.

Scope

This policy applies to all Jeeva AI business units and personnel involved in the selection, engagement, and management of third parties that provide goods or services, including those with access to company data, systems, or facilities.

Roles and Responsibilities

- *Head of IT:* Policy owner; responsible for implementation, maintenance, oversight, and annual review of this policy.
- *Technical Leads:* Identify third-party needs, participate in risk assessments, and ensure compliance with this policy.
- *Procurement leads:* Facilitates due diligence, contract management, and maintains a central inventory of third-party relationships.
- *Legal:* Reviews and approves contractual terms related to risk, compliance, and termination.
- *All Employees:* Must report any third-party risks or incidents to the Head of IT.

Third Party Selection and Due Diligence

A. Risk-Based Vendor Segmentation

- All third parties are categorized into risk tiers (high, medium, low) based on criticality, access to sensitive data, and impact on business operations.
- High-risk (Tier 1) vendors undergo enhanced due diligence, including security, privacy, and compliance check.

B. Due Diligence Process

- Perform initial risk assessments before engagement, evaluating financial stability, security posture, regulatory compliance, and reputation.
- For AI-specific vendors, assess ethical AI practices, transparency, and alignment with Jeeva's AI governance standards.
- Document findings and retain records in the third-party inventory.

Contractual Requirements

- All contracts must clearly define roles, responsibilities, security and privacy requirements, performance metrics, and notification obligations for incidents or breaches.
- Contracts must include provisions for:
    - Approval of subcontractors and sub-processors.

Jeeva AI, Inc.
2708 Wilshire Boulevard #321
Santa Monica, CA 90403, US

- Right to audit and monitor third-party activities.
- Termination rights for non-compliance or material breaches.
- Data protection and confidentiality clauses.

Oversight and Ongoing Monitoring

A. Designated Relationship Owner

- Assign an owner for each third-party relationship to manage communications, oversee performance, and ensure contract compliance.

B. Ongoing Monitoring Activities

- Continuously assess third-party performance and compliance through:
  - Regular risk assessments using questionnaires, security ratings, and compliance checks.
  - Monitoring service level agreements (SLAs) and key performance indicators (KPIs).
  - Tracking and investigating security incidents, data breaches, or operational disruptions.
  - Annual reviews for high-risk vendors, biennial for medium-risk, and triennial for low-risk vendors.

C. AI-Specific Oversight

- Monitor AI vendors for responsible AI practices, transparency, and compliance with evolving regulations.

Issue Management and Escalation

- Establish clear escalation paths for reporting and addressing third-party incidents or breaches.
- Document and investigate all incidents, with corrective actions tracked and reported to management and, if necessary, the board.
- Reassess the relationship and consider termination if risks cannot be adequately mitigated.

Record Keeping and Reporting

- Maintain a centralized inventory of all third-party relationships, risk assessments, contracts, and monitoring activities.
- Provide regular reports to management on third-party risk status, incidents, and remediation efforts.

Policy Review and Maintenance

- The Head of IT will review this policy annually or after any significant incident or regulatory change.
- Updates will be approved by management and communicated to all relevant staff.

Policy Communication

- This policy is distributed to all employees and contractors upon onboarding and is available via the company intranet.
- Training on third-party risk management is mandatory for all relevant personnel.

Approved by: Jeeva AI Management Team
Policy Owner: Head of IT
Next Review Date: Oct 31, 2025