sardine

Acceptable Use

SardineAI Corp. (SardineAI)

May 20, 2026

Table of Contents

Acceptable Use 3
SardineAI Acceptable Use Policy 3
- 1.0 Purpose 3
- 2.0 Scope 3
- 3.0 Policy for Acceptable Use 3
  - 3.1 General Use and Ownership 3
  - 3.2 Prohibited Usage of SardineAI's IT Resources 4
  - 3.3 Email and Communications Activities 5
  - 3.4 Blogging and Social Media 5
  - 3.5 Employee Acknowledgement 6
- 4.0 Enforcement 6
- 5.0 Document Control 6

Acceptable Use

Acceptable use policy is a document stipulating constraints and practices that a user must agree to for access to a corporate network and other organizational assets.

SardineAI Acceptable Use Policy

1.0 Purpose

The purpose of this policy is to outline the acceptable use of SardineAI computing and network resources (IT resources) as well as other organizational assets (information and others). These rules are in place to protect the employee and SardineAI, as inappropriate use exposes SardineAI to risks including cyber attacks, compromise of systems and services, and legal issues.

2.0 Scope

This policy applies to all employees, contractors, consultants, temporary workers, visitors given temporary access to systems, partners, and other workers at SardineAI and its affiliates, including all personnel affiliated with third parties accessing SardineAI's information assets and resources. This policy also applies to all IT resources that are owned or leased by SardineAI. Compliance is mandatory and SardineAI reserves the right to enforce policies, including but not limited to disciplinary procedures and termination of employment.

3.0 Policy for Acceptable Use

3.1 General Use and Ownership

Users of SardineAI's IT Resources are expected to abide by the following guidelines that are built around the underlying principles of acceptable use of organizational assets:

- Comply with all local and applicable international laws.
- Comply with customer's contractual security obligations and requirements.
- Comply with all SardineAI policies, regulations, procedures, and rules.
- Respect and protect the intellectual property rights of SardineAI, its customers and other users within SardineAI.
- Refrain from sharing passwords or accounts with anyone, including trusted friends or family members. Users will be held responsible for any actions performed using their accounts.
- Practice the same level of etiquette in all communication using SardineAI's IT resources as expected in non-electronic communication.
- Respect others when using SardineAI's IT resources.

- Only access files or data if they belong to you or are publicly available, or the owner of the data has permitted you to access them.
- Use corporate e-mail accounts, Internet IDs and web pages for corporate-sanctioned communications.
- Use the Internet/intranet and e-mail judiciously. The use of the Internet/intranet and email may be subject to monitoring for security and/or network management reasons.
- The distribution of any information through the Internet, computer-based services, e-mail, and messaging systems is subject to the scrutiny of the IT team and Security Team. SardineAI reserves the right to determine the suitability of this information.
- While SardineAI's IT department desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of SardineAI.
- The use of SardineAI networks and assets are intended for SardineAI business purposes only.
- Employees must use extreme caution when opening email attachments received from unknown senders, which may contain viruses or other malware.
- All employees must use machines with MDM installed, whole disk encryption enabled and enforced, and have a virus/malware protection installed and enabled.
- Use of biometric features of SardineAI equipment (e.g. Macbook fingerprint reader) is optional and is not required to conduct work. Any employee use of optional biometric features constitutes consent for SardineAI to store and process that employee's biometric data. To opt-out, do not use the optional biometric features of SardineAI equipment.

3.2 Prohibited Usage of SardineAI's IT Resources

Following usages of SardineAI's IT Resources are prohibited. Under no circumstances, an employee of SardineAI is authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing SardineAI-owned resources.

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

- Circumvention of any security measure of SardineAI, its customers or another entity.
- Intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic that substantially hinders others in their use of the network.
- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by SardineAI.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of copyrighted sources and the installation of any

copyrighted software for which SardineAI or the end user does not have an active license is strictly prohibited.

- Reveal or publicize SardineAI's confidential or proprietary information which includes, but is not limited to: financial information, new business and product ideas, marketing strategies and plans, databases and the information contained therein, customer lists, technical product information, computer software source codes, computer/network access codes, and business relationships.
- Visit Internet sites that contain obscene, hateful or any objectionable material unless approved by your manager for business purposes.
- Make or post indecent or harassing remarks, proposals, or materials on the Internet.
- Download any software or electronic files without implementing anti-virus protection measures approved by SardineAI.
- Intentional use, distribution or creation of viruses, worms, or other malicious software.
- Operating a business, usurping business opportunities, organized political activity, conducting activity for personal gain, or other conflicts of interest.
- Implying that the user is representing, giving opinions, or otherwise making statements on behalf of SardineAI without prior authorization or using SardineAI trade names, logos, or trademarks without prior written authorization.
- For business needs and based on approval, if BYOD (Bring Your Own Devices) arrangements are in place i.e. Personally owned workstations or mobile devices are used for business purposes, users shall not create or store confidential or sensitive information on personally owned devices.

3.3 Email and Communications Activities

- Sending unsolicited email or other types of electronic messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (spam).
- Use of unsolicited emails originating from within SardineAI's networks or from other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by SardineAI or connected via SardineAI's network.
- Solicit emails that are unrelated to business activities or for personal gains.
- Send confidential emails without suitable encryption.

3.4 Blogging and Social Media

Blogging and using social media by employees, whether using SardineAI's property and systems or personal computer systems are also subject to the terms and restrictions outlined in this policy. Limited and occasional use of SardineAI's systems to engage in blogging or other social media is acceptable, provided that it is done professionally and responsibly, does not otherwise violate SardineAI's security policies. Blogging or using social media from SardineAI's systems is also subject to monitoring.

- As such, Employees are prohibited from revealing any SardineAI confidential or proprietary information, trade secrets or any other confidential information when engaged in blogging.
- Employees shall not engage in any blogging or social media use that may harm or tarnish the image, reputation or goodwill of SardineAI and any of its employees.
- Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or using social media.
- Employees may also not attribute personal statements, opinions or beliefs to SardineAI when engaged in blogging or using social media.
- If an employee is expressing his or her beliefs or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of SardineAI. Employees assume any risks associated with blogging or using social media.

3.5 Employee Acknowledgement

I have received the Acceptable Use Policy and understand it is my responsibility to read and comply with the policies contained in this document and any revisions made to it. Furthermore, I acknowledge that this document is not a contract of employment.

Employee Name:_____

Date:_____

Signature:_____

4.0 Enforcement

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

5.0 Document Control

Version	Date	Approved By	Notes
2.1	2024-05-20	Bil Corry	Annual review and added enforcement section
2.0	2023-01-11	Bil Corry	Updated Scope, Policy Content including MDM, Violation details, Added document control and Employee Acknowledgement
1.0	2020-11-16	Zahid Shaikh	Initial Policy