Company Name:	Policy Name: **Acceptable Use**
Policy Number: **Acceptable Use Policy 1.0**	Effective Date:
Responsible for Review:	Review Date:

Purpose of Policy

The purpose of this policy is to ensure that employees understand what functions should and should not be performed on **(organization_name)** computers and network to maximize the security of Personally Identifiable Information (PII) and sensitive company data. The policy also provides guidance regarding proper safeguards of PII and sensitive company data when accessing social media sites.

Computer Use

1) To ensure that workstations and other computer systems that may be used to send, receive, store or access PII and sensitive company data are only used in a secure and legitimate manner, all employees must comply with **(organization_name)** Computer Use Policy, a copy of which is attached as Appendix A.

2) **(organization_name)** may provide workstations and other computer systems to employees for the purpose of performing their job functions. Employees shall be responsible for using workstations appropriately in conformance with this Policy.

3) **(organization_name)** may remove or deactivate any employee's user privileges, including but not limited to, user access accounts and access to secured areas, when necessary to preserve the integrity, confidentiality and availability of its facilities, user services, and data.

4) Employees must be assigned and use a unique User Identification and Password.

5) Employees that use **(organization_name)** information systems and workstation assets should have no expectation of privacy. To appropriately manage its information system assets and enforce appropriate security measures, **(organization_name)** may log, review, or monitor any data stored or transmitted on its information system assets.

Appendix A
Computer Use Policy

Introduction

This document provides guidelines for appropriate use of computer facilities and services. It is not a comprehensive document covering all aspects of computer use. It offers principles to help guide employees, and specific policy statements serve as a reference point. It will be modified as new questions and situations arise.

Computers, the Internet and electronic mail (e-mail) are powerful research, communication, commerce and time-saving tools that are made available to employees. The use of this efficient and effective communication tool is critical but, like any tools, computers, the Internet and e-mail have the potential to be used for inappropriate purposes.

Workstations and other computer systems may be provided to employees for the purpose of performing their job functions. Employees shall be responsible for using workstations appropriately in conformance with this Policy.

Policy

The following policies on computer, the Internet and electronic mail usage shall be observed by all employees.

- Users of the Internet and e-mail are to comply with all appropriate laws, regulations and generally accepted Internet etiquette.
- Primary purpose of the Internet and e-mail is to conduct official business.
- Users should identify themselves properly when using the Internet and e-mail, conduct themselves professionally, and be aware that their activities reflect on the reputation and integrity of all employees.
- Each user is individually responsible for the content of any communication sent over or placed on the Internet and e-mail.
- All employees have a responsibility to ensure a respectful workplace. Computer equipment must not be used to visit Internet sites that contain pornographic or sexually explicit information, pictures, or cartoons.
- All employees are to only use their company devices on password-secured wireless networks. Unsecured networks are feeding grounds for hackers and put users and devices at risk.

- Exceptions to this policy are only allowed when pre-approved by supervisors or company management and deemed necessary for official business, research or investigatory work.

The following actions are prohibited. It is unacceptable for employees to:

- Knowingly or intentionally publish, display, transmit, retrieve or store inappropriate or offensive material on any department computer system.
- Create or distribute defamatory, false, inaccurate, abusive, threatening, racially offensive or otherwise biased, discriminatory or illegal material.
- View or distribute obscene, pornographic, profane, or sexually oriented material.
- Violate laws, rules, and regulations prohibiting sexual harassment.
- Engage in any unauthorized activities for personal financial gain.
- Place advertisements for commercial enterprises, including but not limited to, goods, services or property.
- Download, disseminate, store or print materials including articles and software, in violation of copyright laws.
- Download any software, including but not limited to games, screen savers, toolbars or any other browsing tools without the permission of supervisors, company management or IT staff.
- Violate or infringe on the rights of others.
- Conduct business unauthorized by **(organization_name)**.
- Knowingly or intentionally enter financial information, health records, or any sensitive data into ChatGPT that could possibly negatively impact **(organization_name)**.
- Restrict or inhibit other users from using the system or the efficiency of the computer systems.
- Cause congestion or disruption of networks or systems, including distribution of chain letters.
- Transmit incendiary statements, which might incite violence or describe or promote the use of weapons.
- Use the system for any illegal purpose or contrary to company policy or business interests.

- Connect a personal computer to the company network without having the computer checked by IT staff to ensure no threatening viruses / programs infect the company network.
- Monitor or intercept the files or electronic communications of other employees or third parties.
- Hack or obtain access to systems or accounts they are not authorized to use.
- Disclose a Login ID(s) or password to anyone nor allow anyone to access any information system with someone else's Login ID(s) or passwords
- Paste a Login ID(s) or password into ChatGPT without permission from the IT team.
- Use other people's Login ID(s) or passwords to access any information system for any reason.
- Employees are prohibited from using the same passwords between company and non-company accounts.
- Employees are prohibited from accessing any company resources using unauthorized devices including but not limited to laptops, desktops, tablets, and other mobile devices.
- The same passwords are not permitted across multiple company accounts.
- To post any PII or sensitive company data on social network sites, public forums, etc. This includes posting pictures of PII or sensitive company data or pictures of customers without permission.
- Employees shall not remove electronic media that contains PII or confidential or proprietary information unless such removal is authorized by an employee's supervisor or company management.

Any employee who abuses the privilege of their access to e-mail or the Internet in violation of this policy will be subject to corrective action, including possible termination of employment, legal action, and criminal liability.

Note: *Nothing in this policy is meant to, nor should it be interpreted to, in any way limit your rights under any applicable federal, state, or local laws, including your rights under the US National Labor Relations Act to engage in protected concerted activities with other employees to improve terms and conditions of employment, such as wages and benefits.*

Employees will immediately report any activity that violates this agreement to the employee's supervisor, company management or company Security Officer.

I have read, understand, and agree to comply with the foregoing policies, rules, and conditions governing the use of the company computer and telecommunications equipment and services. I understand that I have no expectation of privacy when I use any of the telecommunication equipment or services. I am aware that Internet and e-mail may be subject to monitoring. I am aware that violations of this guideline on appropriate use of the e-mail and Internet systems may subject me to disciplinary action, including termination from employment, legal action and criminal liability.

I further understand that my use of the e-mail and Internet may reflect on the image of the company to our customers, competitors and suppliers and that I have a responsibility to maintain a positive representation of company. Furthermore, I understand that this policy can be amended at any time.

By signing this Agreement, I agree to comply with its terms and conditions. Failure to read this Agreement is not an excuse for violating it. **(organization_name)** may deny access to information systems if this Agreement is not returned signed and dated.

_____	_____
Signature	Date
_____	_____
Requestor's Immediate Supervisor Signature	Date
_____	_____
Access Agreement Approved by (printed name)	Date