



Acceptable Use

Apex Order Pickup Solutions

March 17, 2025

Table of Contents

Table of Contents	2
Acceptable Use	3
Apex Order Pickup Solutions 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 Apex Order Pickup Solutions's IT Resources	4
3.3 Email and Communications Activities	4
3.4 Blogging and Social Media	5

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.

Apex Order Pickup Solutions Acceptable Use Policy

1.0 Purpose

The purpose of this policy is to outline the acceptable use of Apex Order Pickup Solutions's computing and network resources (IT resources) as well as other organizational assets. These rules are in place to protect the employee and Apex Order Pickup Solutions, as inappropriate use exposes Apex Order Pickup Solutions to risks including virus attacks, compromise of systems and services, and legal issues. Any questions regarding this Policy should be directed to the employees direct Manager/Supervisor.

2.0 Scope

This policy applies to employees, contractors, consultants at Apex Order Pickup Solutions, including all personnel affiliated with third parties. This policy also applies to all IT resources owned or leased by Apex Order Pickup Solutions.

3.0 Policy for Acceptable Use

3.1 General Use and Ownership

Users of Apex Order Pickup Solutions's IT resources are expected to abide by the following guidelines 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 information security policies, regulations, procedures, and rules.
- Respect and protect the intellectual property rights of Apex Order Pickup Solutions, its customers and other users within Apex Order Pickup Solutions.
- Shall not be negligent or cause intentional damage to Apex Order Pickup Solutions' property.
- 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.
- Users must maintain confidentiality and exclusive control of authentication credentials (passwords, tokens, certificates) used to access the Company Technology. Credentials must not be shared with others at any time or left in a place where an unauthorized person might find them. If a User has reason to believe that his/her password has been compromised or discovered by another person, the User must immediately inform his/her manager or IT and change his/her password immediately.
- Apply the same level of etiquette in all communication using Apex Order Pickup Solutions's IT resources to all non-electronic communication.
- Respect others when using Apex Order Pickup Solutions's IT resources.
- Only access files or data belonging to you or that are publicly available or where the owner of the data has permitted you to access them.
- Use corporate e-mail accounts, Internet IDs and web pages for corporate communications.
- Use the Internet/intranet and electronic communication judiciously. 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. Apex Order Pickup Solutions reserves the right to determine the suitability of this information.
- While Apex Order Pickup Solutions'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 Apex Order Pickup Solutions.

- Employees must use extreme caution when opening email attachments received from unknown senders, as such email attachments may contain viruses or other malware.

3.2 Prohibited Usage of Apex Order Pickup Solutions's IT Resources

The following usages of Apex Order Pickup Solutions's IT resources are prohibited. Under no circumstances is an employee of Apex Order Pickup Solutions authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Apex Order Pickup Solutions-owned resources.

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

- Circumvention of any security measure of Apex Order Pickup Solutions, its customers or other entities.
- Intentionally interfering with the network's regular operation, including the propagation of computer viruses and sustained high volume network traffic that substantially hinders the network performance. Network(s) include virtual or physical network environments used/operated by Apex Order Pickup Solutions.
- Violations of the rights of any person or organization protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, which includes but not limited to the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Apex Order Pickup Solutions.
- 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 Apex Order Pickup Solutions or the end-user does not have an active license is strictly prohibited.
- Revealing or publicizing Apex Order Pickup Solutions'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.
- Visiting Internet sites that contain obscene, hateful or any objectionable material.
- Access Internet sites for gambling or any illegal activity.
- Store, access, transfer, download, upload, communicate or create any fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, libelous, slanderous, threatening, abusive, defamatory, or otherwise unlawful or inappropriate materials.
- Making or posting indecent remarks, proposals, or materials on the Internet.
- Downloading any software or electronic files without implementing anti-virus protection measures approved by Apex Order Pickup Solutions.
- Intentionally using, distributing or creating viruses, worms, or other malicious software.
- Operating a business, usurping business opportunities, organizing political activity, or conducting activity for personal gain.
- Implying that the user is representing, giving opinions, or otherwise making statements on behalf of Apex Order Pickup Solutions without prior authorization or using Apex Order Pickup Solutions 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 workstations.
- To prevent the introduction of malware and information leakage or data loss in Apex Order Pickup Solutions, portable storage media and personal cloud storage is prohibited unless specifically authorized by the IT Department.

3.3 Email and Communications Activities

- Sending unsolicited email or other types of electronic messages, including sending "junk mail" or other advertising material to individuals who did not specifically request such material (spam).
- Use of unsolicited emails or electronic communications originating from Apex Order Pickup Solutions's networks or from other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Apex Order Pickup Solutions or connected via Apex Order Pickup Solutions's network.
- Soliciting emails or other electronic communications that are unrelated to business activities or for personal gains.
- Use electronic communication to harass other employees and/or other outside individuals or groups.

3.4 Blogging and Social Media

Blogging and using social media by employees, whether using Apex Order Pickup Solutions'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 Apex Order Pickup Solutions's systems to engage in blogging or other social media is acceptable, provided that it is done professionally and responsibly and does not otherwise violate Apex Order Pickup Solutions's security policies. Blogging or using social media from Apex Order Pickup Solutions's systems is also subject to monitoring.

- As such, Employees are prohibited from revealing any Apex Order Pickup Solutions 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 Apex Order Pickup Solutions 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 Apex Order Pickup Solutions 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 Apex Order Pickup Solutions. Employees assume any risks associated with blogging or using social media.