

Acceptable Use Policy (AUP)



Version number	11.0
Last Approved	Feb 25, 2025
Classification	PUBLIC

Overview

The Acceptable Use Policy (AUP) stipulates constraints and practices that Company Personnel must abide by while accessing and using The Company's resources and data, or client data. This policy covers areas which include but are not limited to: hardware, software, email and messaging, data storage, PII, internet, wireless networking, blogging, social media, and third party services.

Applicability

The applicability of this statement falls under purview of the [Security Documentation Overview](#).

Purpose

This Acceptable Use Policy provides guidelines for the use of computing resources and considerations on appropriate use of Company and customer data to ensure compliance with applicable laws and regulations.

Scope

This policy applies to all Personnel working with the Company's data or data provided by the customer for use in providing services.

In the event of conflicting obligations between Company policy and contractual requirements, the more stringent shall be applicable in the handling of customer data.

Acceptable Use Policy

Personnel must use IT Resources in an approved, ethical, and lawful manner in compliance with this AUP and other Company policies and procedures, to avoid damage to The Company and its customers. Personnel must contact a member of the Security Team or Management to report suspected violations of this AUP.

The Company provides access to IT Resources (e.g., desktop computers, laptop computers, servers, smart-phones, networking equipment, etc.) to facilitate the completion of Company business. Care must be taken to ensure the safety and security of these resources.

Personnel who have been issued IT Resources are responsible for the physical security of those resources, regardless of where they are used (e.g., Company offices, residences, hotels, conference rooms, cars, airports, etc.). Personnel should adhere to a “clear desk/clear screen” protocol.

IT Resources and Company data stored are Company owned assets. Any damage or theft to Company assets found to be caused by gross negligence of the person to whom the asset was assigned will be recovered by The Company from the Personnel responsible.

Prohibitions

Generally prohibited activities when using IT Resources include, but are not limited to:

- Stealing or copying electronic files without permission.
- Unauthorized software installation on company assets; installing software that has not been assessed and approved.
- Establishing personal shares on (or otherwise sharing access to) Company assets.
- Stealing Company-owned property.
- Violating the rights of any person or company protected by copyright, trade secret, patent, intellectual property laws, or similar laws or regulations; including, but not limited to installing or distributing “pirated” software or other software products that are not appropriately licensed for use by The Company.
- Exporting software, technical information, or encryption software or technology in violation of international or regional export control laws.
- Revealing account passwords to others or allowing the use of an account by anyone other than the individual to whom it is assigned. (This includes family and other household members when work is being done at home.)

- The use of “shared” or “group” Accounts to access Company or client assets is prohibited except for approved use cases.
- Performing non work related activities that may degrade the performance of networks and systems (e.g., playing electronic games, excessive use of internet based audio and video streaming programs, etc.).
- Performing activities intended to circumvent security or the access controls including the possession or use of hardware or software tools intended to defeat software copy protection, discover passwords, identify security vulnerabilities, decrypt files, or compromise information security by any other means.
- Breaching security or “disrupting” network communications. (For purposes of this section, “disrupting” includes, but is not limited to: network sniffing, ping floods, packet spoofing, denial of service, and forging routing information for malicious purposes.) Security breaches include, but are not limited to: intentionally accessing data or logging into a server or account to which Personnel are not expressly authorized (unless these actions are within the scope of regular duties); writing, copying, executing, or attempting to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of (or access to) any Company computer, network, or information.
- Accessing the Company network remotely via access methods not approved by the Company.
- Using Company IT Resources to promote or maintain a personal or private business, or for personal gain.
- Using Company IT Resources to perform any other activities that are in violation of Company policies.

Hardware

Use of Personally-Owned Hardware

Personnel must NOT connect non-Company-owned computers or computing devices to any Company networks (except to designated “Guest Networks”). This includes computers owned by an individual or another corporation; networking hardware such as routers, hubs, switches, wireless access points, etc.; or any other computing device. This restriction applies to computers physically connected to a Company network (in a Company office) as well as those connected remotely (VPN). All exceptions must be approved by the VP Information Security.

Personnel may use personally-owned computers to connect to Company webmail including Smartphones via ActiveSync. However, Personnel should not connect to webmail from computers that they do not control (e.g., public terminals, kiosks, etc.) except in emergency situations where no other method of communication is possible. Personnel may not use personally-owned external storage devices to capture, transport, or store data of any kind from Company-owned computer systems.

Software

All software must be obtained from official Company sources. Introduction of any software into The Company's computing environments must be approved by Corporate IT Operations. Approved software and SaaS can be found via the [LTG Software & SaaS List](#).

Use of Personally-Owned Software

To protect IT Resource integrity, Personnel must not use personally owned software on IT Resources without the approval of Corporate IT Operations. This includes purchased applications; shareware; freeware; downloads from bulletin boards, the Internet, Company Intranet, FTP sites, local area networks (LANs) or wide area networks (WANs); and other personally owned or controlled software.

Monitoring

To ensure adherence to software usage policies and related federal laws and statutes, The Company reserves the right to monitor software installation and usage on all Company IT Resources, as well as any privately owned computers when used to conduct Company business.

- Corporate IT Operations conducts ongoing scans of all IT Resources for installed software and licensing information. Any unlicensed or unauthorized software is removed (or licensed appropriately).

Protection of Intellectual Property

To ensure the integrity of Company developed software, all personnel must abide by the requirements for protecting (and the proper usage and disclosure of) proprietary Company data, as stated in The Company's [Data Classification Policy](#).


Proper Data Storage


Clients and partners entrust The Company with sensitive information related to their businesses. The nature of this custodianship requires strict confidentiality; any disclosure of sensitive information could adversely affect The Company's business relationships, position in the technology community, and competitive advantage.

Personnel are required to protect Confidential Information with good judgement and the highest ethical standards as well as guard against its inadvertent disclosure. More specifically, Personnel are required to store Confidential Information only in secured locations (on secured servers) and not on portable devices.

Portable Media

To ensure that Confidential Information is not placed at unnecessary risk, The Company restricts the use of portable storage devices (i.e., flash drives, external USB drives, DVD burners, etc.) Personnel are prevented from writing to portable media on Company owned devices.

 Reading from portable media is allowed.

 Personnel whose job role requires writing data to portable media are exempt. Any other personnel wishing to write to portable media must have approval from two lines of management and the Chief Information Security Officer. (Contact [Security](#) for instructions on acquiring an exception.)

Whenever writing data to portable media, full-disk encryption (via BitLocker) is required.

Cloud Storage

The Company embraces using cloud solutions, including cloud storage. However, not all cloud storage solutions are equal. They vary widely both in security features and their providers' underlying security practices.

To protect clients' privacy as well as to reduce the risk of any data "leakage", The Company requires the use of **Company-administered cloud solutions** (only) when writing data to the cloud.

Internet

Access to the Internet is available to Personnel whose duties require it for the conduct of Company business. Since Internet activities may be monitored, all Personnel accessing the Internet should have no expectation of privacy.

The Company provides Internet access to facilitate the conduct of Company business. Occasional and incidental personal Internet use is permitted if it does not interfere with the work of Personnel, the Company's ability to perform its mission, and the conditions outlined in this policy.

Prohibited activities while using the Internet include, but are not limited to:

- Browsing pornographic or hate-based web sites; posting, sending, or acquiring sexually explicit or sexually oriented material, hate-based material, or other material determined to be prohibited (except where required by duties for monitoring or policy enforcement, for which management approval is required)
- Browsing hacker or cracker websites; posting, sending, or acquiring hacker or cracker-related material, or other material that The Company has determined to be prohibited (except where required by duties for monitoring or policy enforcement, for which management approval is required)
- Participating in newsgroups or discussion websites using a Company email address (even for work-related discussions)
- Posting or sending sensitive information outside the corporation without management authorization
- Using Instant Messaging applications or protocols other than those managed by Corporate IT Operations is strictly prohibited.
- Installing or using any 'peer-to-peer' file sharing software
- Installing or using any 'distributed computing' software
- Engaging in excessive use of internet-based streaming audio or video programs (except where required for completion of duties, organizational communication functions, or training purposes)
- Initiating data transfer (e.g., FTP, SCP, Telnet, SSH, VPN, etc.) with foreign systems or networks unless required to perform Company sanctioned functions (e.g., receiving patch updates, uploading debug files, etc.). Inbound VPN and SSH connections initiated from foreign networks must be approved by Security prior to attempting connection.
- Posting or hosting non-Company related commercial announcements or advertising material on Company computer information systems or networks
- Using Company resources to maintain a personal or private business
- Receiving news feeds or pushing data updates on subjects that are not related to The Company, your job, or career enhancement
- Using the Internet to perform any other activities which are in violation of Human Resources policies

Wireless Networking

Acceptable Wireless Use

The use of wireless networking is acceptable for conducting Company business in the following situations:

- Connecting to Company networks while attending Company functions outside normally assigned work areas (e.g., meetings and interviews).
- Connecting to Company networks while at other venues (e.g., hotels, external meetings, etc.) where no other means of network access is available.
- Connecting at home, where security measures have been implemented to secure and limit access to the wireless network (WPA or WPA2 wireless encryption)

❌ Wireless networking must not be used to access production networks.

All connections to Company computing resources (other than Webmail) made from home or other non-Company locations (where The Company's wired or wireless network is not available) must be made via VPN.

❌ In the absence of a VPN connection, the transmission of Company data over unsecured Wi-Fi is prohibited.

Prohibited Wireless Use

Prohibited activities when using Wireless networking include, but are not limited to:

- Connecting wireless access points to Company-owned networks. (Wireless access points may only be connected to Company-owned networks by Corporate IT Operations.)
- Using PC-to-PC wireless connections

❌ Connecting Company-owned devices to a wireless network for non-business use is strictly prohibited.


ℹ All exceptions to the Wireless Networking provisions of this policy must be approved by Corporate IT Operations management.

Mobile Devices

Mobile devices are highly attractive targets for theft and attempted compromise. Care must be taken to secure mobile devices not only because of their monetary value, but also because of the sensitive data stored therein.

Physical Security

Specific actions must be taken by all Personnel who have a Company-issued mobile computing device (e.g., desktop, laptop, tablet, smartphone, etc.) or who are temporarily using a “shared” Company mobile device.

 Personnel must secure all mobile devices when they are not being used.

- All mobile devices acquired for (or on behalf of) The Company are deemed Company property.
- All Personnel issued a mobile device are responsible for the security of their mobile device, regardless of if it is used in the office, at a place of residence, or in any other location (e.g., hotel, conference room, car, or airport).
- Mobile devices (excluding desktops) that are not taken home after working hours must be secured in a locked cabinet, drawer, or secure office. Leaving a mobile device in a docking station or on a desk is **NOT** acceptable.
- While traveling, mobile devices must not be left unattended at any time while powered on. If left in a hotel room, they must be powered off and not left in plain sight, but placed in a concealed location (e.g., drawer, closet, under the bed, etc.). If provided, hotel room safes or secure cabinets must be used to store mobile devices or mobile device hard drives.
- When traveling, mobile devices must not be checked in with luggage. Keep mobile devices with you at all times.
- If a mobile device must be left in a vehicle it must be secured in a trunk (in the case of cars) or behind the seat with locked doors (in the case of trucks).
- Mobile devices (excluding desktops²) that will not be used for several days must be locked out of sight in a secure cabinet or safe.

Security Controls

Subverting installed security software or security settings on any Company device is strictly prohibited (except where required by Personnel’s normal duties, for which Corporate IT Operations Team or Security Team approval is required).

Sensitive Data on Mobile Devices

Personally Identifiable Information (“PII”: e.g., Social Security Numbers, credit card numbers, driver’s license numbers, etc.) must never be stored on mobile devices that do not have company sanctioned full disk encryption software installed. (This includes USB drives.)


Responsibility

Mobile devices are company owned assets; therefore, any damage or theft found to be caused by reasons other than normal “wear and tear” (e.g., misuse or neglect in taking proper security precautions) will be recovered by The Company from the Personnel to whom the device was issued.

Access

General

- Personnel must never leave mobile devices unlocked. Screen-locking mechanisms must be engaged on unattended devices. (Disconnecting from any active VPNs is also recommended.)
- Mobile devices that connect to company email systems must have an idle “time-out” lock, with:
 - A maximum 15 minute idle time-out
 - A minimum 4-digit PIN authentication

 Finger swipe PIN systems are not an acceptable means of authentication.

Home Access

- Mobile devices that are taken home must not be left connected to the Internet when not in use.
- Mobile devices that are taken home must not be utilized for anything other than company business. (They must not be left unattended where family members or visitors have access to them.)

Mobile Phone Numbers

Personnel may be issued a telephone number (or be allowed to provide their own telephone number) for use on their Company-issued Smartphone. Upon assignment, these phone numbers become the property of The Company; Personnel rescind any and all rights to ownership of these numbers.

Ensuring Compliance

The Company owns all IT Resources, and these resources remain the property of The Company while assigned to Personnel for their use in conducting Company business. Use of Company IT Resources constitutes the Personnel's consent for The Company to monitor,

inspect, audit, collect, or remove any information without permission or further notice. Personnel will be informed as to what use is acceptable and what is prohibited. Any infraction of Company acceptable use policies constitutes a policy violation, for which Personnel will be held personally accountable.

Additional Information

Additional information related to *Disciplinary Actions, Exceptions* and *Questions* can be found in the [Security Documentation Overview](#).

Document control

i This policy is only controlled in its live, digital format. Any other format or export of this policy is an uncontrolled version of this document

Document Owner	@Art Machado	
Author(s)	@Art Machado @PauGordon @angelinahakilmer	
Required Approver(s) and Approval Date	@Art Machado - VP Information Security	Feb 25, 2025
Review cycle	ANNUAL	
Next review date	Feb 24, 2026	

Version History

Date	Author(s)	Version	Changes
Feb 25, 2025	@Paul Gordon	11.0	Annual review
Nov 01, 2024	@angelina.kilmer	10.4	Updated Policy classification from Confidential to Public

Mar 28, 2024	@Art Machado @Sarah Zwicker (Unlicensed) @Paul Gordon	10.3	Annual Review
Dec 4, 2023	@Sarah Zwicker (Unlicensed)	10.2	Updated Security email from @peoplefluent.com to @ltgplc.com
May 16, 2023	@Sarah Zwicker (Unlicensed) & @Art Machado	10.1	Updated Password Administration section
Feb 23, 2023	@Sarah Zwicker (Unlicensed) & @Art Machado	10.0	Annual review + Logo change
Mar 16, 2022	@Sarah Zwicker (Unlicensed) & @Art Machado	9.9	Title change for VP InfoSec, Annual Review (no major changes noted)
Jun 15, 2021	@Sarah Zwicker (Unlicensed) & @Art Machado	9.8	Updated Scope and Purpose
Mar 10, 2021	@Sarah Zwicker	9.7	Changed owner, updated Overview

	(Unlicensed)		
Feb 9, 2021	@Sarah Zwicker (Unlicensed)	9.6	Reformatting, linked policies
Jan 26, 2021	@John Cole	9.5	Annual review
11/20/2020	John Cole	9.4	Changed owner