# Why is the Acceptable Use Policy (AUP) important?

This policy establishes the rules for anyone who accesses or uses Kirkhill's computers, applications, data, or networks. Everyone is responsible to follow these rules to protect themselves, as well as the organization. Failure to follow the practices outlined in this policy can result in serious financial and reputational damage to the organization.

# Who does this policy apply to?

This policy applies to anyone and everyone who interacts with Kirkhill’s information systems, including NMC systems. For example, this policy applies to Kirkhill and NMC:

* Employees
* Contractors
* Consultants
* Temporary employees
* Internal or external contacts
* Visitors
* All roles and levels of the organization

# Which systems does this policy apply to?

This policy applies to all types of information systems and communications owned or operated by Kirkhill, Inc., NMC, and any other Kirkhill subsidiaries. For example, this policy applies to Kirkhill and NMC:

* Computers
* Phones
* Networks
* Communications
* Electronic files and data
* Mobile phones and devices
* Internet usage
* Email
* Software applications

Be sure to download this policy and refer to it often. Violating this policy can cause serious trouble to you as well as to the organization.

# Rules and Guidelines

## General

### Privacy: Kirkhill will monitor all computer and network activities, including but not limited to, email, internet activity, mobile device activity, phone calls, chat messages, etc. No Kirkhill employees, nor any other user of Kirkhill systems, should make any assumption of privacy when using company systems, applications, or networks.

### Abuses and violations: Violating any law, regulation, or security policy, or using or accessing any computer systems in a manner which puts the company’s systems, information, customers, or business interests at risk, either intentionally, or inadvertently through negligent or irresponsible behavior, is strictly prohibited. Circumventing, bypassing, disabling, or in any way weakening the security protections of any company systems is strictly prohibited.

### Reporting violations: Employees are required to report any suspected or actual security breaches involving cloud services immediately to the IT department. This includes any unauthorized access, data leakage, or compromise of company information, or violation of company security policy. Employees have a responsibility to immediately report the theft, loss, or unauthorized disclosure of sensitive information, as well as the loss or theft of any physical device containing such information.

## Computer Network

### Company-owned devices: Employees are required to use only company-provided devices for all work-related activities, and for connecting to any company networks, services, or applications. This includes accessing Kirkhill-provided cloud applications, applications which employees access directly on the internet, such as Infor CSI and Office 365. This also includes VPN connections, accessing email on iPhones or from laptops. All these types of connections to company resources require the use of company owned laptops, mobile phones, or tablets.

### Strong passwords: When accessing Kirkhill systems, employees are required to utilize strong passwords. The same password must never be used for more than one application or system. Passwords must be at least 8 characters in length and contain at least one upper-case letter, one lower case letter, and one number or symbol. Passwords must be changed every 90 days.

### Login with Phone or Token (MFA): In addition to the use of strong passwords, all users are required to verify their identity with a smartphone app or a hardware token. Email verification is acceptable only if phone or token is not supported. Text or SMS message verification is not an acceptable form of authentication. Employees must never provide their verification code to anyone, not even to IT or to their manager. Employees must never click to accept a phone or token verification prompt which they do not recognize or which they did not intentionally initiate, particularly when receiving numerous unexpected prompts (MFA fatigue). Employees must lock or protect their token, badge or smartphone when unattended to prevent unauthorized persons from using them to gain access to facilities or systems.

### Password storage: All passwords must be stored only in the company approved password management application. Storing passwords in Excel sheets, sticky notes, documents, or in any other locations or systems which are not authorized for such purpose is prohibited.

### Unauthorized software: Introduction, installation, or usage of any unauthorized, unlicensed, or risky software is strictly prohibited.

### Password secrecy: Revealing your account password to others or allowing use of your account by others is prohibited. Even for taking time off or cross training, you may not share your password or your account with any coworkers or manager, even for legitimate business reasons. Contact IT if coworkers need to perform your job duties in your absence.

### Remote work: Employees must be approved to access corporate systems remotely based on their job role and duties. Employees requiring remote access must be assigned company devices. Employees working remotely, using company systems in remote locations, or connecting to company applications or data from remote locations must adhere to KHWI 4.8.16 and IT-004 regarding control and usage of company systems while traveling.

### Unauthorized devices: Connecting any unauthorized devices such as USB drives, hard drives, storage devices, mobile devices, or wireless devices, to company computers or networks is prohibited. All portable or mobile devices must be owned and approved by Kirkhill before connecting to any system.

**Blogging and social media:** Using Kirkhill’s property and systems for social media, blogging, or any digital communication in a manner that violates this Policy, harms Kirkhill’s interests, reveals sensitive or restricted information, harms or tarnishes the company image, or violates Non-Discrimination and Anti-Harassment policies, is prohibited.

## Email

### Email risk: The company receives thousands of dangerous emails daily which puts the company at risk of cyber-attacks and financial fraud. Threats such as phishing are the primary method used by criminals to gain access to company systems, and in the vast majority of cases, it’s the employee who clicks and triggers the attack. To protect the company from these risks, employees must learn the skills to detect them, and exercise extreme caution every day, when reading or opening email messages.

### Training: All users of corporate email systems are required to complete mandatory training, provided by the company, regarding safe email practices. Management and HR will be informed of any employees who are overdue on training.

### Employee responsibility: It is the responsibility of all email users to be skilled at recognizing and avoiding dangerous email threats, and to actively participate in identifying these threats and in protecting the organization. Employees are responsible to inform the IT department if they need additional training on safe email practices, or if they encounter an email which may pose a risk to the organization.

**Abusive or inappropriate behavior:** Distributing unsolicited email messages, "junk mail", or advertising material to individuals who did not request such content through email. Engaging in any form of harassment via messaging through offensive language. Unauthorized alteration or forging of email.

## Sensitive Information

### NMC Mexico: NMC employs individuals who may not be US persons. Transfer or sharing of technical or financial data with any individual or entity who may not be a “US person” requires training to ensure no regulations or laws will be violated. Contact the Export Control department before transferring information which may relate to any government application. Employees must exercise caution when using email or Teams, or when collaborating with NMC counterparts, to ensure government technical or financial information is not shared accidentally.

### Legal and regulatory frameworks: Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property is prohibited. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Kirkhill or the end user does not have an active license is strictly prohibited.

### Export Control: Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws is prohibited.

### Information types: Kirkhill identifies and controls sensitive information in accordance with all applicable laws and regulations. All sensitive information must be handled, marked, and protected in accordance with Kirkhill’s Information Control Plan. Employees may access, use, transfer, or share sensitive information only to the extent it is authorized, approved, and necessary to fulfill their assigned job duties. All types of sensitive information are limited in who may access or receive it, and employees must refer to management or the IT department for appropriate authorization. Sensitive information includes but is not limited to:

* Proprietary Information (PI)
* Intellectual Property (IP)
* Confidential Information (CI)
* Personally Identifiable Information (PII)
* Personal Health Information (PHI)
* Covered Defense Information (CDI)
* Controlled Unclassified Information (CUI)
* Federal Contract Information (FCI)

## Cloud Applications (Internet Hosted Software)

The public internet provides access to countless applications which allow an individual to create an account and begin using the applications, often even for free or for a small monthly payment, without any knowledge or consent by the company’s IT department. This unauthorized or unsanctioned use of public cloud applications is often referred to as “Shadow IT” and poses a major risk to the organization.

Cloud applications are online platforms, operated by third-party companies, which can be directly accessed over the public internet, allowing us to use software or store data without installing them on our devices. Examples include Kirkhill services like Infor CSI Office 365, and Outlook email. The risk comes from cloud applications which are not sanctioned by Kirkhill, but which users are able to use regardless because they are publicly accessible over the internet. These unsanctioned internet applications are particularly dangerous because employees can intentionally or unintentionally transfer sensitive company information to them, potentially exposing the organization to legal or financial losses.

**IT Approval:** All cloud services must undergo a review and be approved by IT before they are used for company proprietary information, sensitive information, critical business functions, technical data, or any similar sensitive functions.

### Prohibited Cloud Usage: Any applications or services available on the public internet are expressly prohibited from handling any company sensitive or proprietary information unless expressly approved and authorized by the IT Department. File sharing sites like Dropbox.com or Boxx.com may be blocked to prevent transfers of sensitive company information. Communication and messaging sites such as Slack.com and Gmail.com, and personal email accounts of any kind are strictly prohibited because dangerous attachments can be downloaded directly to company computers bypassing all company email filters and firewalls.

### ChatGPT and other public AI services: Publicly accessible AI services offer significant productivity and automation benefits. They also pose very real and unique risks to the organization. It is prohibited to enter any text, prompts, questions, documents, sheets, images, or information of any kind which is not intended for release to the general public. All information entered into these applications is equivalent to releasing the information to the public, and is subject to all regulatory and legal restrictions, as well as company policies regarding sensitive data.

**Microsoft Office, Email, Teams:** Microsoft Office 365 provides Kirkhill employees with Office applications, email, Teams collaboration, and an expansive list of other applications. The Microsoft cloud platform is authorized to handle all forms of Kirkhill sensitive information providing that users exercise caution to ensure that the information is only accessible by authorized personnel. Never share technical or financial information related to any defense customer or contract in any email, Teams chat or group which is accessible by NMC employees who are non-US citizens. Always be aware if camera or microphone are on. Be aware of risk of screen sharing and do not accidentally expose sensitive data. Never accept chat messages from non-Kirkhill employees or unidentified persons.

**Infor CloudSuite Industrial (ERP):** Infor CSI is authorized to handle all forms of Kirkhill sensitive information. The application is configured to prevent any unauthorized transfer of information between Kirkhill and NMC databases.

**Customer Portals/Exostar:** Each customer collaboration portal such as Exostar is governed by its own use policy, terms, and conditions. All users must be approved for access and must understand and comply with the terms and conditions of the portals they use.

**GovFTP/ShareTru:** GovFTP (aka ShareTru) is authorized to handle all forms of Kirkhill sensitive information. Users must be approved before being granted access and must understand and comply with all regulatory requirements before sharing any technical information with outside parties.

# Violations of Policy

### Improper Usage: Violating any law, regulation, or security policy, or using or accessing any computer systems in a manner which puts the company’s systems, information, customers, or business interests at risk, either intentionally, or inadvertently through negligent or irresponsible behavior, is strictly prohibited.

### Legal and Regulatory frameworks: Kirkhill computer systems and data are governed and controlled under a broad range of legal and regulatory frameworks. This policy is designed to clarify the policies and procedures necessary for employees to utilize company information systems in a legal and compliant matter.

### Disciplinary Action: Violating this policy may result in disciplinary action, up to and including termination and/or criminal prosecution.