Acceptable Use Policy, version 1.0.0

Status: ☐ Working Draft ☐ Approved ☒ Adopted
Document Owner: Picerne IT Department
Last Review Date: December 2021

Acceptable Use Policy

Purpose

The purpose of the Picerne Real Estate Group Acceptable Use Policy is to establish acceptable practices regarding the use of Picerne Real Estate Group **Information Resources** in order to protect the confidentiality, integrity and availability of information created, collected, and maintained.

Audience

The Picerne Real Estate Group Acceptable Use Policy applies to any individual, entity, or process that interacts with any Picerne Real Estate Group **Information Resource**.

Contents

Policy

Acceptable Use

- Personnel are responsible for complying with Picerne Real Estate Group policies when using Picerne Real Estate Group information resources and/or on Picerne Real Estate Group time. If requirements or responsibilities are unclear, please seek assistance from the IT Department.
- Personnel must promptly report the theft, loss, or unauthorized disclosure of Picerne Real Estate Group **confidential** or **internal information** to the IT Department.
- Personnel should not purposely engage in activity that may
    - harass, threaten, or abuse others;
    - degrade the performance of Picerne Real Estate Group **Information Resources**;
    - deprive authorized Picerne Real Estate Group personnel access to a Picerne Real Estate Group **Information Resource;**
    - obtain additional resources beyond those allocated;
    - or circumvent Picerne Real Estate Group computer security measures.
- Personnel should not download, install, or run security programs or utilities that reveal or exploit weakness in the security of a system. For example, Picerne Real Estate Group personnel should not run password cracking programs, packet sniffers, port scanners, or any other non-approved programs on any Picerne Real Estate Group **Information Resource**.
- All inventions, intellectual property, and proprietary information, including reports, drawings, blue prints, software codes, computer programs, data, writings, and technical information, developed on Picerne Real Estate Group time and/or using Picerne Real Estate Group **Information Resources** are the property of Picerne Real Estate Group.
- Use of encryption should be managed in a manner that allows designated Picerne Real Estate Group personnel to promptly access all data.
- Picerne Real Estate Group **Information Resources** are provided to facilitate District business and should not be used for personal financial gain.
- Personnel are expected to cooperate with incident investigations, including any federal or state investigations.
- Personnel are expected to respect and comply with all legal protections provided by patents, copyrights, trademarks, and intellectual property rights for any software and/or materials viewed, used, or obtained using Picerne Real Estate Group **Information Resources**.
- Personnel should not intentionally access, create, store or transmit material which Picerne Real Estate Group may deem to be offensive, indecent, or obscene.

Access Management

- Access to information is based on a "need to know".
- Personnel are permitted to use only those network and host addresses issued to them by Picerne Real Estate Group IT and should not attempt to access any data or programs contained on Picerne Real Estate Group systems for which they do not have authorization or explicit consent.
- All remote access connections made to internal Picerne Real Estate Group networks and/or environments must be made through approved, and Picerne Real Estate Group-provided, virtual private networks (VPNs).
- Personnel should not divulge any access information to anyone not specifically authorized to receive such information.
- Personnel must not share their Picerne Real Estate Group authentication information, including:
    - Account passwords,
    - Personal Identification Numbers (PINs),
    - Security Tokens (i.e. Smartcard),
    - Access cards and/or keys,
    - Digital certificates,
    - Similar information or devices used for identification and authentication purposes.
- Lost or stolen access cards, security tokens, and/or keys must be reported to the person responsible for **Information Resource** physical facility management as soon as practical.
- A service charge may be assessed for access cards, security tokens, and/or keys that are lost, stolen, or are not returned.

Authentication/Passwords

- All personnel are required to maintain the confidentiality of personal authentication information.
- Any group/shared authentication information must be maintained solely among the authorized members of the group.
- All passwords, including initial and/or temporary passwords, must be constructed, and implemented according to the following Picerne Real Estate Group rules:
    - Must meet all requirements established in the Picerne Real Estate Group Authentication Standard, including minimum length, complexity, and rotation requirements.
    - Must not be easily tied back to the account owner by using things like: user name, social security number, nickname, relative's names, birth date, etc.
    - Should not include common words, such as using dictionary words or acronyms.
    - Should not be the same passwords as used for non-business purposes.
- Password history must be kept to prevent the reuse of passwords.
- Unique passwords should be used for each system, whenever possible.
- User account passwords must not be divulged to anyone.
- Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with Picerne Real Estate Group, if issued.
- If the security of a password is in doubt, the password should be changed immediately.
- Personnel should not circumvent password entry with application remembering, embedded scripts or hard coded passwords in client software.

Clear Desk/Clear Screen

- Personnel should log off from applications or network services when they are no longer needed.
- Personnel should log off or lock their workstations and laptops when their workspace is unattended.
- Confidential or internal information should be removed or placed in a locked drawer or file cabinet when the workstation is unattended and at the end of the workday if physical access to the workspace cannot be secured by other means.
- Personal items, such as phones, wallets, and keys, should be removed or placed in a locked drawer or file cabinet when the workstation is unattended.
- File cabinets containing **confidential information** should be locked when not in use or when unattended.
- Physical and/or electronic keys used to access **confidential information** should not be left on an unattended desk or in an unattended workspace if the workspace itself is not physically secured.
- Laptops should be either locked with a locking cable or locked away in a drawer or cabinet when the work area is unattended or at the end of the workday if the laptop is not encrypted.
- Passwords must not be posted on or under a computer or in any other physically accessible location.
- Copies of documents containing **confidential information** should be immediately removed from printers and fax machines.

Data Security

- Personnel should use approved encrypted communication methods whenever sending confidential information over public computer networks (Internet).
- Confidential information transmitted via USPS or other mail service must be secured in compliance with the Information Classification and Management Policy.
- Only authorized **cloud computing applications** may be used for sharing, storing, and transferring **confidential** or **internal information**. Use of personal accounts is prohibited.
- Information must be appropriately shared, handled, transferred, saved, and destroyed, based on the information sensitivity.
- Personnel should not have confidential conversations in public places or over insecure communication channels, open offices, and meeting places.
- **Confidential information** must be transported either by an Picerne Real Estate Group employee or a courier approved by IT Management.
- All electronic media containing confidential information must be securely disposed. Please contact IT for guidance or assistance.
- Data on endpoint computers is not backed up by Picerne IT. Critical data should always be stored on Picerne Real Estate Group file servers, or cloud storage approved by Picerne IT Management.

Email and Electronic Communication

- Auto-forwarding electronic messages outside the Picerne Real Estate Group internal systems is prohibited.
- Electronic communications should not misrepresent the originator or Picerne Real Estate Group.

- Personnel are responsible for the accounts assigned to them and for the actions taken with their accounts.
- Accounts must not be shared without prior authorization from Picerne Real Estate Group IT, with the exception of calendars and related calendaring functions.
- Employees should not use personal email accounts to send or receive Picerne Real Estate Group **confidential information**.
- Any personal use of Picerne Real Estate Group provided email should not:
    - Involve solicitation.
    - Be associated with any political entity, excluding the Picerne Real Estate Group sponsored PAC.
    - Have the potential to harm the reputation of Picerne Real Estate Group.
    - Forward chain emails.
    - Contain or promote anti-social or unethical behavior.
    - Violate local, state, federal, or international laws or regulations.
    - Result in unauthorized disclosure of Picerne Real Estate Group **confidential information**.
- Personnel should only send **confidential information** using secure electronic messaging solutions.
- Personnel should use caution when responding to, clicking on links within, or opening attachments included in electronic communications.
- Personnel should use discretion in disclosing **confidential** or **internal information** in Out of Office or other automated responses, such as employment data, internal telephone numbers, location information or other sensitive data.

Hardware and Software

- All hardware must be formally approved by IT Management before being purchased or connected to Picerne Real Estate Group networks.
- Software installed on Picerne Real Estate Group equipment must be approved by IT Management and installed by or under guidance from Picerne Real Estate Group IT personnel.
- All Picerne Real Estate Group assets taken off-site should be physically secured at all times.
- Personnel traveling to a High-Risk location, as defined by FBI and Office of Foreign Asset control, must contact IT for approval to travel with corporate assets.
- Employees should not allow family members or other non-employees to access Picerne Real Estate Group **Information Resources**.

Internet

- The Internet must not be used to communicate Picerne Real Estate Group **confidential** or **internal information**, unless the confidentiality and integrity of the information is ensured and the identity of the recipient(s) is established.
- Use of the Internet with Picerne Real Estate Group networking or computing resources must only be used for business-related activities.
- Unacceptable use of the internet by employees includes, but is not limited to:
    - Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via Picerne Real Estate Group email service
    - Using computers to perpetrate any form of fraud, and/or software, film or music piracy
    - Stealing, using, or disclosing someone else's password without authorization

  - Downloading, copying or pirating software and electronic files that are copyrighted or without authorization
  - Sharing confidential material, trade secrets, or proprietary information outside of the organization
  - Hacking
  - Sending or posting information that is defamatory to the company, its products/services, colleagues and/or customers
  - Introducing malicious software onto the company network and/or jeopardizing the security of the organization's electronic communications systems
  - Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities
  - Passing off personal views as representing those of the organization

- All sites and downloads may be monitored and/or blocked by Picerne Real Estate Group IT management if they are deemed to be harmful and/or not productive to business
- Access to the Internet from outside the Picerne Real Estate Group network using a Picerne Real Estate Group owned computer must adhere to all of the same policies that apply to use from within Picerne Real Estate Group facilities.

Endpoint Protection (Anti-Virus & Malware)

- All Picerne Real Estate Group owned and/or managed **Information Resources** must use the Picerne Real Estate Group IT management approved endpoint protection software and configuration.
- All non-Picerne Real Estate Group owned workstations and laptops must use Picerne Real Estate Group IT management approved endpoint protection software and configuration, prior to any connection to a Picerne Real Estate Group **Information Resource**.
- The endpoint protection software must not be altered, bypassed, or disabled.
- Each email gateway must utilize Picerne Real Estate Group IT management approved email virus protection software and must adhere to the Picerne Real Estate Group rules for the setup and use of this software, which includes, but is not limited to, scanning of all inbound and outbound emails.
- Controls to prevent or detect the use of known or suspected malicious websites must be implemented.
- All files received over networks or from any external storage device must be scanned for malware before use.
- Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to Picerne Real Estate Group IT Support.

Mobile Devices and Bring Your Own Device (BYOD)

- The use of a **personally-owned mobile device** to connect to the Picerne Real Estate Group network is a privilege granted to employees only upon formal approval of IT Management.
- All **personally-owned** laptops and/or workstations must have approved virus and spyware detection/protection software along with personal firewall protection active.

- Mobile devices that access Picerne Real Estate Group email must have a PIN or other authentication mechanism enabled.
- Picerne Real Estate Group **confidential information** should not be stored on any personally-owned **mobile device**.
- Theft or loss of any **mobile device** that has been used to create, store, or access **confidential** or **internal information** must be reported to the Picerne Real Estate Group Security Team immediately.
- All **mobile devices** must maintain up-to-date versions of all software and applications.
- All personnel are expected to use **mobile devices** in an ethical manner.
- Jail-broken or rooted devices should not be used to connect to Picerne Real Estate Group **Information Resources**.
- Picerne Real Estate Group IT Management may choose to execute "remote wipe" capabilities for **mobile devices** without warning.
- In the event that there is a suspected incident or breach associated with a **mobile device**, it may be necessary to remove the device from the personnel's possession as part of a formal investigation.
- All mobile device usage in relation to Picerne Real Estate Group **Information Resources** may be monitored, at the discretion of Picerne Real Estate Group IT Management.
- Picerne Real Estate Group IT support for personally-owned **mobile devices** is limited to assistance in complying with this policy. Picerne Real Estate Group IT support may not assist in troubleshooting device usability issues.
- Use of **personally-owned** devices must be in compliance with all other Picerne Real Estate Group policies.
- Picerne Real Estate Group reserves the right to revoke **personally-owned mobile device** use privileges in the event that personnel do not abide by the requirements set forth in this policy.
- Texting or emailing while driving is not permitted while on company time or using Picerne Real Estate Group resources. Only hands-free talking while driving is permitted, while on company time or when using Picerne Real Estate Group resources.

Physical Security

- Photographic, video, audio, or other recording equipment, such as cameras in mobile devices, is not allowed in secure areas.
- Personnel must badge in and out of access-controlled areas. Piggy-backing, door propping and any other activity to circumvent door access controls are prohibited.
- Visitors accessing card-controlled areas of facilities must be accompanied by authorized personnel at all times.
- Eating or drinking are not allowed in data centers. Caution must be used when eating or drinking near workstations or information processing facilities.

Privacy

- Information created, sent, received, or stored on Picerne Real Estate Group **Information Resources** are not private and may be accessed by Picerne Real Estate Group IT employees at any time, under the direction of Picerne Real Estate Group executive management and/or Human Resources, without knowledge of the user or resource owner.
- Picerne Real Estate Group may log, review, and otherwise utilize any information stored on or passing through its **Information Resource** systems.

- Systems Administrators, Picerne Real Estate Group IT, and other authorized Picerne Real Estate Group personnel may have privileges that extend beyond those granted to standard business personnel. Personnel with extended privileges should not access files and/or other information that is not specifically required to carry out an employment related task.

Removable Media

- The use of **removable media** for storage of Picerne Real Estate Group information must be supported by a reasonable business case.
- All **removable media** use must be approved by Picerne Real Estate Group IT prior to use.
- **Personally-owned removable media** use is not permitted for storage of Picerne Real Estate Group information.
- Personnel are not permitted to connect **removable media** from an unknown origin without prior approval from the Picerne Real Estate Group IT.
- Confidential and internal Picerne Real Estate Group information should not be stored on **removable media** without the use of encryption.
- The loss or theft of a **removable media** device that may have contained Picerne Real Estate Group information must be reported to the Picerne Real Estate Group IT.

Social Media

- Communications made with respect to social media should be made in compliance with all applicable Picerne Real Estate Group policies.
- Personnel are personally responsible for the content they publish online.
- Creating any public social media account intended to represent Picerne Real Estate Group, including accounts that could reasonably be assumed to be an official Picerne Real Estate Group account, requires the permission of the Picerne Real Estate Group Communications Departments.
- When discussing Picerne Real Estate Group or Picerne Real Estate Group -related matters, you should:
    - Identify yourself by name,
    - Identify yourself as an Picerne Real Estate Group representative, and
    - Make it clear that you are speaking for yourself and not on behalf of Picerne Real Estate Group, unless you have been explicitly approved to do so.
- Personnel should not misrepresent their role at Picerne Real Estate Group.
- When publishing Picerne Real Estate Group-relevant content online in a personal capacity, a disclaimer should accompany the content. An example disclaimer could be; “The opinions and content are my own and do not necessarily represent Picerne Real Estate Group’s position or opinion.”
- Content posted online should not violate any applicable laws (i.e. copyright, fair use, financial disclosure, or privacy laws).
- The use of discrimination (including age, sex, race, color, creed, religion, ethnicity, sexual orientation, gender, gender expression, national origin, citizenship, disability, or marital status or any other legally recognized protected basis under federal, state, or local laws, regulations, or ordinances) in published content that is affiliated with Picerne Real Estate Group will not be tolerated.
- Confidential information, internal communications and non-public financial or operational information may not be published online in any form.

- Personal information belonging to customers may not be published online.
- Personnel approved to post, review, or approve content on Picerne Real Estate Group social media sites must follow the Picerne Real Estate Group Social Media Procedures.

VoiceMail

- Personnel should use discretion in disclosing **confidential** or **internal information** in voicemail greetings, such as employment data, internal telephone numbers, location information or other sensitive data.
- Personnel should not access another user's voicemail account unless it has been explicitly authorized.

Incidental Use

- As a convenience to Picerne Real Estate Group personnel, incidental use of **Information Resources** is permitted. The following restrictions apply:
  - Incidental personal use of electronic communications, Internet access, fax machines, printers, copiers, and so on, is restricted to Picerne Real Estate Group approved personnel; it does not extend to family members or other acquaintances.
  - Incidental use should not result in direct costs to Picerne Real Estate Group.
  - Incidental use should not interfere with the normal performance of an employee's work duties.
  - No files or documents may be sent or received that may cause legal action against, or embarrassment to, Picerne Real Estate Group or its customers.
- Storage of personal email messages, voice messages, files and documents within Picerne Real Estate Group **Information Resources** must be nominal
- All information located on Picerne Real Estate Group **Information Resources** are owned by Picerne Real Estate Group may be subject to open records requests and may be accessed in accordance with this policy.

Waivers

Waivers from certain policy provisions may be sought following the Picerne Real Estate Group Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	December 2021		Forrest Vaughn	Document Origination