ACCEPTABLE USE POLICY

Table of Contents

Purpose

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

Audience

The Ames Construction Acceptable Use Policy applies to any individual, entity, or process that interacts with any Ames Construction **Information Resource**.

Acceptable Use

- Personnel are responsible for complying with Ames Construction policies when using Ames Construction information resources and/or on Ames Construction time. If requirements or responsibilities are unclear, please seek assistance from Ames IT Support.
- Personnel must promptly report the theft, loss, or unauthorized disclosure of Ames Construction **confidential** or **internal information** to the Security Committee.
- Personnel should not purposely engage in activity that may
    - harass, threaten, impersonate, or abuse others;
    - degrade the performance of Ames Construction **Information Resources**;
    - deprive authorized Ames Construction personnel access to an Ames Construction **Information Resource;**
    - obtain additional resources beyond those allocated; or
    - circumvent Ames Construction 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, Ames Construction personnel should not run password cracking programs, packet sniffers, port scanners, or any other non-approved programs on any Ames Construction **Information Resource**.
- All inventions, intellectual property, and proprietary information, including reports, drawings, blueprints, software codes, computer programs, data, writings, and technical information, developed on Ames Construction time and/or using Ames Construction **Information Resources** are the property of Ames Construction.
- Use of encryption should be managed in a manner that allows designated Ames Construction personnel to promptly access all data.
- Ames Construction **Information Resources** are provided to facilitate company 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 Ames Construction **Information Resources**.
- Personnel should not intentionally access, create, store or transmit material which Ames Construction 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 Ames Construction IT and should not attempt to access any data or programs contained on Ames Construction systems for which they do not have authorization or explicit consent.
- All remote access connections made to internal Ames Construction networks and/or environments must be made through approved, and Ames Construction-provided, Citrix/virtual private networks (VPNs).
- Personnel should not divulge any access information to anyone not specifically authorized to receive such information include IT support personnel.

- Personnel must not share their (authentication information, including:
    - Account passwords,
    - Personal Identification Numbers (PINs),
    - Security Tokens (i.e. Smartcard),
    - Multi-factor authentication information
    - 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 Ames Construction rules:
    - Must meet all requirements established in the Ames Construction 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. Ames Construction support personnel and/or contractors should never ask for user account passwords.
- Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with Ames Construction, 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.

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**.
- 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 Ames Construction 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.

Email and Electronic Communication

- Auto-forwarding electronic messages outside the Ames Construction internal systems is prohibited.
- Electronic communications should not misrepresent the originator or Ames Construction.
- 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 Ames Construction IT, with the exception of calendars and related calendaring functions.
- Employees should not use personal email accounts to send or receive Ames Construction **confidential information**.
- Any personal use of Ames Construction provided email should not:
    - Involve solicitation.
    - Be associated with any political entity, excluding the Ames Construction sponsored PAC.
    - Have the potential to harm the reputation of Ames Construction.
    - 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 Ames Construction **confidential information**.
    - Otherwise violate any other policies that have been approved and adopted.
- Personnel should only send **confidential information** using approved 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 and abide by the purchasing standard before being connected to Ames Construction networks.
- Software installed on Ames Construction equipment must be approved by IT Management, abide by the purchasing standard and installed by Ames Construction IT personnel.
- All Ames Construction 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 Ames Construction **Information Resources**.

Internet

- The Internet must not be used to communicate Ames Construction **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 Ames Construction networking or computing resources must only be used for business related activities. Unapproved activities include, but are not limited to:
    - Recreational games,
    - Streaming media,
    - Personal social media,
    - Accessing or distributing pornographic or sexually oriented materials,
    - Attempting or making unauthorized entry to any network or computer accessible from the Internet.
    - Or otherwise violate any other policies that have been approved and adopted.
- Access to the Internet from outside the Ames Construction network using a Ames Construction owned computer must adhere to all of the same policies that apply to use from within Ames Construction facilities.

Mobile Devices and Bring Your Own Device (BYOD)

- Ames Construction does not allow **personally-owned mobile devices** to connect to the Ames Construction internal network.
- Mobile devices that access Ames Construction email must have a PIN or other authentication mechanism enabled.
- Confidential data should only be stored on devices that are encrypted in compliance with the Ames Construction Encryption Standard.
- Ames Construction **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 Ames Construction 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 Ames Construction **Information Resources**.
- Ames Construction IT Management may choose to execute “remote wipe” capabilities for **mobile devices** without warning (see Mobile Device Email Acknowledgement).
- 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 Ames Construction **Information Resources** may be monitored, at the discretion of Ames Construction IT Management.
- Ames Construction IT support for personally-owned **mobile devices** is limited to assistance in complying with this policy. Ames Construction IT support may not assist in troubleshooting device usability issues.
- Use of **personally-owned** devices must be in compliance with all other Ames Construction policies.
- Ames Construction reserves the right to revoke **personally-owned mobile device** use privileges in the even 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 Ames Construction resources. Only hands-free talking while driving is permitted, while on company time or when using Ames Construction resources.

Physical Security

- Photographic, video, audio, or other recording equipment, such as cameras and cameras in mobile devices, is not allowed in secure areas.
- Personnel must badge in and out of access-controlled areas. Piggy-backing, tailgating, 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 Ames Construction **Information Resources** are not private and may be accessed by Ames Construction IT employees at any time, under the direction of Ames Construction executive management and/or Human Resources, without knowledge of the user or resource owner.
- Ames Construction may log, review, and otherwise utilize any information stored on or passing through its **Information Resource** systems.
- Systems Administrators, Ames Construction IT, and other authorized Ames Construction 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 Ames Construction information must be supported by a reasonable business case.
- All **removable media** use must be approved by Ames Construction IT prior to use and followed the established registration process.
- **Personally-owned removable media** use is not permitted for storage of Ames Construction information.
- Personnel are not permitted to connect **removable media** from an unknown origin without prior approval from the Ames Construction IT.
- Confidential and internal Ames Construction information should not be stored on **removable media** without the use of encryption.
- All removable media must be stored in a safe and secure environment.
- The loss or theft of a **removable media** device that may have contained Ames Construction information must be reported to the Ames Construction IT.

Security Training and Awareness

- All new personnel must complete an approved security awareness training class prior to, or at least within 30 days of, being granted access to any Ames Construction **Information Resources**.
- All personnel must be provided with and acknowledge they have received and agree to adhere to the Ames Construction Information Security Policies before they are granted to access to Ames Construction **Information Resources**.
- All personnel must complete the annual security awareness training.

Social Media

- Communications made with respect to social media should be made in compliance with all applicable Ames Construction policies.
- Personnel are personally responsible for the content they publish online.
- Creating any public social media account intended to represent Ames Construction, including accounts that could reasonably be assumed to be an official Ames Construction account, requires the permission of the Ames Construction Communications Departments.

- When discussing Ames Construction or Ames Construction -related matters, you should:
    - Identify yourself by name,
    - Identify yourself as an Ames Construction representative, and
    - Make it clear that you are speaking for yourself and not on behalf of Ames Construction, unless you have been explicitly approved to do so.
- Personnel should not misrepresent their role at Ames Construction.
- When publishing Ames Construction-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 Ames Construction'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 Ames Construction 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 Ames Construction social media sites must follow the Ames Construction Social Media Management Procedures.

Voice Mail

- 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 Ames Construction 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 Ames Construction approved personnel; it does not extend to family members or other acquaintances.
    - Incidental use should not result in direct costs to Ames Construction.
    - 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, Ames Construction or its customers.
- Storage of personal email messages, voice messages, files and documents within Ames Construction **Information Resources** must be nominal
- All information located on Ames Construction **Information Resources** are owned by Ames Construction may be subject to open records requests and may be accessed in accordance with this policy.

Ames Construction

ACCEPTABLE USE POLICY

I acknowledge that I have received training and have access to Ames's Acceptable Use Policy.

I acknowledge this policy by my dated signature below. I understand that this agreement is a condition of employment and the form will be made part of my personnel file.

_____

Employee Name (Print)

How do you want to be known at Ames? (Ex:Mike instead of Michael)

_____

Employee Signature

_____

Date