# Acceptable Use Guideline for Guests – Dakota Electric Association

**Last Review Date: April 1, 2022**

**Last Reviewed By: DEA IT-Security Team**

## Purpose

The purpose of the Dakota Electric Association (DEA) Acceptable Use Guideline for Guests is to establish acceptable practices regarding the use of DEA Information Resources, in order to protect the confidentiality, integrity, and availability of information created, collected, and maintained.

## Scope

The DEA Acceptable Use Guideline for Guests applies to any individual, entity, or process that interacts with any DEA information resource. Guests include vendors, partners, contractors, and other non-employees.

## Guideline

### Acceptable Use

- All DEA Guests are responsible for complying with DEA guidelines when using DEA information resources and/or on DEA time. If requirements or responsibilities are unclear, please seek assistance from the DEA Help Desk or Information Services management.
- DEA Guests must promptly report the theft, loss or unauthorized disclosure of DEA confidential or internal information to the DEA Help Desk or Information Services management.
- DEA Guests should not purposely engage in activity that may
    - harass, threaten or abuse others;
    - degrade the performance of DEA information resources;
    - deprive authorized DEA employee access to a DEA information resource(s)**;**
    - obtain additional resources beyond those allocated;
    - or circumvent DEA computer security measures.
- DEA Guests should not download, install or run security programs or utilities that reveal or exploit weakness in the security of a system. For example, DEA Guests should not run password cracking programs, packet sniffers, port scanners, or any other non-approved programs on any DEA 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 DEA time and/or using DEA information resources are the property of DEA.
- Use of encryption should be managed in a manner that allows designated DEA employees to promptly access all data.

- DEA information resources are provided to facilitate company business and should not be used for personal financial gain.
- DEA Guests are expected to cooperate with incident investigations, including any federal or state investigations.
- DEA Guests 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 DEA information resources.
- DEA Guests should not intentionally access, create, store or transmit material which DEA may deem to be offensive, indecent or obscene.

## Access Management

- Access to information is based on a "need to know".
- DEA Guests are permitted to use only those network and IP addresses issued to them by DEA Information Services and should not attempt to access any data or programs contained on DEA systems for which they do not have authorization or explicit consent.
- All remote access connections made to internal DEA networks and/or environments must be made through approved, and DEA-provided, virtual private networks (VPNs), or otherwise secure connections.
- DEA Guests should not divulge any access information to anyone not specifically authorized to receive such information.
- DEA Guests must not share their DEA 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 Help Desk as soon as practicable.

## Authentication/Passwords

- All DEA Guests 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 DEA rules:
    - Must meet all requirements established in the DEA Password Guideline, 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 in order 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. DEA Information Services staff 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 DEA, if issued.
- If the security of a password is in doubt, the password should be changed immediately.
- DEA Guests should not circumvent password entry with application remembering, embedded scripts or hard coded passwords in client software.

## Clear Desk/Clear Screen

- DEA Guests should log off from applications or network services when they are no longer needed.
- DEA Guests 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.
- All laptops should utilize full desktop encryption.
- 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

- DEA Guests 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 DEA Data Classification Guideline.
- 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.

- DEA Guests 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 DEA employee or a courier approved by DEA Information Services management.
- All electronic media containing confidential information must be securely disposed. Please contact DEA Help Desk for guidance or assistance.

## Email and Electronic Communication

- Auto-forwarding electronic messages outside the DEA internal systems is prohibited.
- Electronic communications should not misrepresent the originator or DEA.
- DEA Guests 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 DEA Information Services management.
- DEA Guests should not use personal email accounts to send or receive DEA confidential information.
- Any personal use of DEA provided email should not:
    - Involve solicitation.
    - Be associated with any political entity.
    - Have the potential to harm the reputation of DEA.
    - 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 DEA confidential information.
- DEA Guests should only send confidential information using secure electronic messaging solutions.
- DEA Guests should use caution when responding to, clicking on links within, or opening attachments included in electronic communications.
- DEA Guests 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 DEA Information Services management before being connected to DEA networks.
- Software installed on DEA equipment must be approved by DEA Information Services management and installed by DEA information services staff.
- All DEA assets taken off-site should be physically secured at all times.
- DEA Guests should not allow family members or other non-employees to access DEA Information Resources.

## Internet

- The Internet must not be used to communicate DEA 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 DEA 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.
- Access to the Internet from outside the DEA network using a DEA owned computer must adhere to all of the same policies that apply to use from within DEA facilities.

## Mobile Devices and Bring Your Own Device (BYOD)

- The use of a personally-owned mobile device to connect to the DEA network is a privilege granted to guests only upon formal approval of DEA Information Services management.
- All personally-owned (vendor/business-owned) laptops and/or workstations must have virus and spyware detection/protection software along with personal firewall protection active.
- Mobile devices that access DEA 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 DEA Encryption Standard.
- DEAconfidential 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 DEAIT-Security Team immediately.
- All mobile devices must maintain up-to-date versions of all software and applications.
- All guests are expected to use mobile devices in an ethical manner.
- Jail-broken or rooted devices should not be used to connect to DEA Information Resources.
- DEA Information Services management may choose to execute “remote wipe” capabilities for mobile devices if deemed necessary to protect DEA assets.
- 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 guests’ possession as part of a formal investigation.
- All mobile device usage in relation to DEAInformation Resources may be monitored, at the discretion of DEA Information Services management.
- DEA Information Services staff support for personally-owned mobile devices is limited to assistance in complying with this policy. DEA Information Services staff support may not assist in troubleshooting device usability issues.
- Use of personally-owned devices must be in compliance with all other DEA guidelines.

- DEA reserves the right to revoke personally-owned mobile device use privileges in the event that guests 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 DEA resources. Only hands-free talking while driving is permitted, while on company time or when using DEA resources.

**Physical Security**

- Photographic, video, audio or other recording equipment, such as cameras in mobile devices, is not allowed in secure areas.
- DEA Guests must use appropriately assigned security cards for access in and out of 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 employees 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 DEA Information Resources are not private and may be accessed by DEA Information Services staff at any time, under the direction of DEA executive management and/or Human Resources, without knowledge of the user or resource owner.
- DEA may log, review, and otherwise utilize any information stored on or passing through its Information Resource systems.
- Systems Administrators, DEA IT-Security team, and other authorized DEA employees may have privileges that extend beyond those granted to standard business employees.

**Removable Media**

- The use of removable media for storage of DEA information must be supported by a reasonable business case.
- All removable media use must be appropriately scanned and receive acceptable approval by DEA Information Services staff prior to use.
- Personally-owned removable media use is not permitted for storage of DEA information.
- DEA Guests are not permitted to connect removable media from an unknown origin, without appropriate scanning and prior approval from DEA Information Services management.
- Confidential and internal DEA 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 DEA information must be reported to the Help Desk immediately.

## Social Media

- Communications made with respect to social media should be made in compliance with all applicable DEA guidelines and policies.
- DEA Guests are personally responsible for the content they publish online.
- Creating any public social media account intended to represent DEA, including accounts that could reasonably be assumed to be an official DEA account, requires the permission of DEA Information Services management.
- When discussing DEA or DEA -related matters, you should:
    - Identify yourself by name,
    - Identify yourself and your role, in relation to DEA and
    - Make it clear that you are speaking for yourself and not on behalf of DEA, unless you have been explicitly approved to do so.
- DEA Guests should not misrepresent their role at DEA.
- When publishing DEA -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 DEA'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 DEA 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 employees or DEA-customers may not be published online.
- Only guests with proper approval will post or maintain content on DEA social media sites.

## Voice Mail

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

## Incidental Use

- As a convenience to DEAguests, 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 DEA approved employees; it does not extend to family members, other acquaintances, or non-employees.
    - Incidental use should not result in direct costs to DEA.

    - Incidental use should not interfere with the normal performance of a guests work duties.
    - No files or documents may be sent or received that may cause legal action against, or embarrassment to, DEA or its customers.
- Storage of personal email messages, voice messages, files and documents within DEA Information Resources must be limited and within reason.
- All information located on DEA Information Resources are owned by DEA may be subject to open records requests, and may be accessed in accordance with this policy.

**Exception**

Exception requests from guideline provisions may be made to DEA Information Services management.

**Enforcement**

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.