

Contractor Information Security Access Agreement (CISAA) and Acceptable Use Policy For Contractors of the Department for Aging and Rehabilitative Services (DARS)

Acceptable Use Policy

I understand that any use of electronic communications tools owned or provided by the Commonwealth of Virginia is limited to business purposes only, and I agree to abide by all applicable Commonwealth of Virginia Policies, Standards, and Guidelines. These Policies, Standards, and Guidelines includes, but are not limited to the Commonwealth of Virginia, Information Technology Resource Management (ITRM) Standard SEC501, Information Security Standard.

I also understand that I am responsible for maintaining the confidentiality, privacy, and security of all Protected Health Information (PHI) in my custody. This includes ensuring my compliance with all Health Insurance Portability and Accountability Act (HIPAA) provisions relevant to PHI, and I will consult the Contractor's HIPAA/Privacy Officer if I have any questions regarding HIPAA Data Privacy.

Business Use

DARS and Contractor provided electronic communications tools are provided to facilitate the effective and efficient conduct of the Commonwealth's business. Users may be permitted access to the Internet and electronic communications tools to assist in the performance of their jobs. Some users may also be permitted to access and use social media to conduct Contractor business. Each Contractor may adopt its own policy setting forth with specificity the work-related purposes for which such equipment and access are provided.

Personal Use

Personal use means use that is not job-related. In general, incidental and occasional personal use of the Commonwealth's electronic communications tools including the Internet is permitted as long as the personal use does not interfere with the user's productivity or work performance, does not interfere with any other employee's productivity or work performance, and does not adversely affect the efficient operation of the Commonwealth's systems and networks. Personal use of social media that refers to any aspect of the work environment shall be done in a responsible and professional manner.

User Requirements

General Requirements

When using electronic communications tools, social media, or Internet access, employees must:

- Use the Internet, electronic communications tools, and social media only in accordance with the Contractor's policy;
- Abide by and maintain the security protocols and conditions (including safeguarding of passwords) under which they are granted access to such media;
- Check with the appropriate Contractor staff prior to downloading or accessing a file or document if the source of the file or other circumstances raises any doubts about its safety or security;
- Be respectful of the Contractor's organization, other employees, customers, vendors, and others when posting and communicating information. Users should be sensitive to referring to or including others in their communications and posts and should be aware of any associated potential liabilities. Users may desire to obtain consent internal approval or authorization prior to communicating or posting information about the work place.

Business Use Requirements

When using electronic communications tools, social media, or Internet access, employees must:

- Use their accurate identities and state their affiliation when using electronic communications or social media for business purposes.
- Ensure the security of sensitive or confidential information when communicating electronically or posting the information on internal or external websites including social media.
- Ensure information is accurate prior to posting on social media sites, state or the Contractor's websites, or other electronic media sites. If it is discovered that information is inaccurate after posting, users should work to quickly correct the errors.

Personal Use Requirements

When using electronic communications tools, social media or Internet access for personal use, employees must:

- Be clear that their communication or posting is personal and is not a communication of the Contractor's or the Commonwealth when using electronic communications or social media for personal use, including personal use of social media outside of the work environment. For example:
 - Users should use their personal email addresses and not those related to their positions with the Commonwealth when communicating or posting information for personal use.
 - When appropriate to ensure a user's personal views are not viewed as official Commonwealth of Virginia communications, users may use a disclaimer when posting opinions or views for personal use such as, "The views expressed on this (website, blog, social media site) are my own and do not reflect the views of my employer or of the Commonwealth of Virginia."

Prohibited Activities

Certain activities are prohibited when using the Commonwealth's Internet and electronic communications media or using social media in reference to the work environment. Prohibited activities include, but are not limited to:

- Using, sharing, or knowingly permitting the use of assigned logon id(s) and password(s) for any purpose other than those required to perform authorized employment functions.
- Using any logon id and password that has not been expressly assigned to me or authorized for my use.
- Transmitting unencrypted data classified as sensitive relative to confidentiality or integrity by any method, including the Contractor's email systems, except by fax.
- Automatically forwarding the Contractor's email to external mail systems, for example, an employee's personal Yahoo email account.
- Storing sensitive data on non-network storage devices, unless the data is encrypted or the Contractor's Information Security Officer (ISO) has provided written permission. Non-network storage devices include any non-networked storage media, including flash drives, CDs/DVDs, or other external storage media.

- Posting any data classified as sensitive with respect to confidentiality on a public website, ftp server, drive share, bulletin board or any other publicly accessible medium unless a written exception is approved by the Contractor's Information Security Officer.
- Tampering with security controls configured on the Contractor's workstations.
- Installing personal or proprietary software on the Contractor's computer systems.
- Adding, removing, or modifying the Contractor's system hardware unless performed in the course of my assigned job duties.
- Connecting unprotected personal devices to PCs, laptops, or handheld devices, except in accordance with the Contractor's policies.
- Streaming audio or video for non-business purposes.
- Any use that is in violation of applicable local, state, and federal law.
- Accessing, uploading, downloading, transmitting, printing, posting, or storing information with sexually explicit content as prohibited by law (see Code of Virginia §2.2-2827).
- Accessing, uploading, downloading, transmitting, printing, posting, or storing fraudulent, threatening, obscene, intimidating, defamatory, harassing, discriminatory, or otherwise unlawful messages or images.
- Installing or downloading computer software, programs, or executable files contrary to the Virginia Information Technology Agency's (VITA) Information Security Policy, Standards, and Guidelines.
- Accessing, uploading, downloading, transmitting, printing, communicating, or posting access-restricted Contractor information, proprietary Contractor's information, sensitive state data or records, or copyrighted materials in violation of the Contractor's or state policy.
- Using proprietary Contractor information, state data or records, and social media to locate the Contractor's customers for personal reasons.
- Posting information or sending electronic communications such as email using another's identity.
- Permitting a non-user to use the electronic communications equipment for purposes of communicating the message of some third party individual or the Contractor.
- Posting photos, videos, or audio recordings taken in the work environment without written consent.
- Using Contractor's logos without written consent.
- Texting, emailing, or using hand-held electronic communications devices while operating a state vehicle.
- Any other activities designated as prohibited by the Contractor.

DARS and Contractor Responsibilities and Requirements

DARS and the Contractor have the following responsibilities and requirements related to this policy.

Monitor Usage

No user shall have any expectation of privacy in any message, file, image or data created, sent, retrieved, received, or posted in the use of the Commonwealth’s equipment and/or access. DARS and the Contractor have a right to monitor any and all aspects of electronic communications and social media usage. Such monitoring may occur at any time, without notice, and without the user’s permission.

In addition, except for exemptions under the Act, electronic records may be subject to the Freedom of Information Act (FOIA) and, therefore, available for public distribution.

Acknowledgements

I acknowledge that the information contained in the DARS computer systems constitutes proprietary and confidential information and agree not to disclose any such information for non-DARS business purposes. If I observe any incidents of non-compliance with the terms of this agreement by any other user, I agree to report them to my supervisor and designated security officer immediately.

I acknowledge that I understand the preceding terms and provisions and that I accept the responsibility of adhering to the same.

I understand that no user shall have any expectation of privacy in any message, file, image, or data created, sent, retrieved, received, or posted in the use of the Commonwealth’s equipment and/or access. DARS and the Contractor have a right to monitor any and all aspects of electronic communications and social media usage. Such monitoring may occur at any time, without notice, and without my permission.

By signing or electronically acknowledging this agreement, I understand that it is my responsibility to read and abide by this policy, even if I do not agree with it. I acknowledge that any infractions of these agreements and/or policies may result in removal of system access and disciplinary action, up to and potentially including termination of employment. If I have any questions about the policy, I understand that I need to ask my supervisor for clarification.

Individual: _____

Supervisor: _____

Date: _____

Supervisor: I certify that the individual has completed the required security awareness training required by the Department for Aging and Rehabilitative Services:

Date: _____ Initials: _____