Policy and Procedure

Virginia Department of Agriculture and Consumer Services

Number 10.1

SUBJECT: **ETHICAL USE OF AGENCY INFORMATION AND COMPUTING RESOURCES**

Date: January 2, 1995

Revision: November 1, 2017

Effective: November 1, 2017

APPROVAL: Sandra J. Adams

Purpose

It is the purpose of this policy to protect citizen and business information, to protect the Department of Agriculture and Consumer Services' (VDACS) information assets, and to expand upon the Virginia Department of Human Resource Management (DHRM) Policy 1.75 – Use of Electronic Communications and Social Media policy.

Scope

This policy is applicable to all Virginia Department of Agriculture and Consumer Services (VDACS) employees, contractors, vendors, and other individuals granted access to VDACS' Information Systems; collectively known as "System Users" or "Users".

System requests covered under this standard include COV (Commonwealth of Virginia) network accounts, Outlook email accounts, remote access, vendor-supplied software access, and Oracle database access.

Roles

This policy is formatted to focus on responsibilities of employees in the following categories: ***"All Users"***, ***"Remote Users"***, ***"Mobile Device Users"***, ***"Supervisors and Managers"***, ***"System Owners"***, ***"Data Owners"*** , ***"System Administrators"***, and ***Information Systems Staff***. Users will be included in multiple categories based on their role.

Definition of Terms

"Information resources" include paper files, facsimile machines, electronic mail and reports and documents, both written and computer generated.

"Information Security Officer" (ISO) – Agency security representative

"Security Incident" a warning that there may be a threat to information or computer security. Threats can be identified by unauthorized access to a system, and can include a denial of service attack, website defacement, malicious code such as Trojans or worms, threat or harassment via electronic medium and intentional misuse of systems.

"Sensitive data" means any data the compromise of which with respect to confidentiality, integrity, or availability could have a material adverse effect on VDACS interests, the conduct of agency programs, or the privacy to which individuals are entitled. Protection of sensitive data may be required for legal or ethical reasons, for issues pertaining to personal privacy, or for proprietary considerations.

Sensitive data includes, but is not limited to:

- Personal information that can lead to identity theft if exposed, e.g. social security number, passport number, credit or debit card number.
- Health information that reveals a person's health condition or history of health services.
- Client information such as proprietary product formulas, trade secrets, open investigation information, or other information that may be exempt from release pursuant to the Virginia Freedom of Information Act.

"Social media" includes blogs, wikis, podcasts, social networks, photograph and video hosting websites, crowd sourcing, and new technologies as they evolve. (Common are Facebook, Twitter, LinkedIn, YouTube, etc.)

- Business Use- Social media used to conduct or enhance agency business. Approved users are permitted access to the Internet and computer resources to assist in the performance of their jobs. (See VDACS Policy 10.3, Business Use of Social Media.)
- Personal Use- Social media that is not job-related, done on the employee's personal time in a responsible and professional manner that does not adversely affect the agency. It should be consistent with the state's values, standards, and policies.

"VDACS computing resource" includes, but is not limited, to any of the following VDACS or Commonwealth of Virginia resources: computers, hand-held computing devices, peripherals, networks, software, data, applications, computer rooms, and computer-related supplies. (Collectively "VDACS computing resources.")

"VDACS issued device" means any VDACS computing resource as well as a VDACS issued phone or VDACS issued tablet. (Collectively "VDACS issued devices.") "VDACS issued device" does not include a personal phone for business, except when a personal phone is used to conduct business activities through a VDACS computing resource.

General Requirements Related to System Access

All system access (new, change, or termination) must be requested via the VDACS Access Request System. A link to the VDACS Access Request System is available on InSite (agency intranet) home page.

Requests for password resets for any agency-owned system (e.g. Oracle accounts) must be made via the VDACS Access Request System. Requests for email, network, and VPN accounts must be made through the VITA Customer Care Center (VCCC).

Access to all VDACS systems and data will be based on the principle of least privilege, which means that an employee will be given only the privileges that are necessary to perform his/her job duties.

Account access levels and privileges must be based on pre-defined roles associated with system functionality. Exceptions must be approved by the agency Information Security Officer (ISO).

New users of any VDACS system will be provided a unique initial password, delivered in a secure and confidential manner that the user must change upon first use.

At least two individuals are required to have administrative accounts to each VDACS system to provide for continuity of operations.

Responsibilities and Requirements

All Users

A "user" is any person who has been granted access to a VDACS computing resource.

All Users Must

- Acknowledge that:
  - All information, data, messages, files, images, or other products maintained in paper filing systems, stored on a VDACS issued device, or sent or retrieved over the Internet using a VDACS issued device, are the property of the Commonwealth of Virginia.
  - VDACS issued devices are intended for business use and personal use is not allowed, except where described in this policy.
  - Users have no expectation of privacy while using a VDACS issued device.
  - All use of a VDACS issued device will be monitored and used in the prosecution of unlawful behavior or otherwise as VDACS

determines, including but not limited to any violation of VDACS or DHRM policies.
    - Non-disclosure of information applies to all agency confidential or sensitive data, not just data on information systems.
- Follow all security guidelines, processes, and procedures provided by the VDACS Information Systems office and the Commonwealth of Virginia.
- Use only the computers, accounts, files, and systems that the user has been approved to use.
- Complete Security Awareness training requirements annually.
- Report any security incident or equipment theft verbally and by email to the ISO and user's supervisor as soon as it is detected. The ISO can be reached at Deborah.Nickerson@vdacs.virginia.gov, (804)786-0489, (804)921-6786 or at (804) 874-6242.
- Alert supervisor if any security requirement is inhibiting work. Users must not attempt to bypass any security requirement.
- Encrypt any email message that contains sensitive data.
- Protect sensitive data by encrypting it.
- Use only encrypted USB drives and encrypted external hard drives.
- Lock their computer when away and it is not visible. To lock press the Windows key and "L" key simultaneously.
- Use only the following information in an email signature:

  Name and Title
  Virginia Department of Agriculture & Consumer Services
  Address
  City, State Zip
  Business telephone number

  Abbreviated versions of the above information are allowed. Licensure or professional designations with name or title and relative to position are allowed. Simple, professional text should be used.

  Do not use special fonts, colors, backgrounds and graphics, which may be blocked by many email clients and mobile devices. Agency authorized promotional logos (Virginia's Finest, Virginia Grown) are allowed. Inspirational quotes or phrases or tag lines are not allowed.

- Use only the Attorney General approved confidentiality statement on emails:

  "The information in this email and any attachments may be confidential and privileged. Access to this email by anyone other than the intended addressee is unauthorized. If you are not the intended recipient (or the employee or agent responsible for delivering this information to the intended recipient) please notify the sender by reply email and immediately delete this email and

any copies from your computer and/or storage system. The sender does not authorize the use, distribution, disclosure or reproduction of this email (or any part of its contents) by anyone other than the intended recipient(s).

No representation is made that this email and any attachments are free of viruses. Virus scanning is recommended and is the responsibility of the recipient."

- Back up work product on the computing device at least monthly.
- Protect VDACS issued devices from magnets, liquids, food, or other similar hazards.
- Connect VDACS issued devices to the Commonwealth of Virginia network at least every 14 days for a minimum of four hours to receive updates and patches to software.
- Change all default passwords on installed software.
- Use a complex password for VDACS computing resources as required by the system or device.
- Maintain exclusive control and use of their passwords for any VDACS issued device or systems.
- Immediately change their password for any VDACS issued device or system and notify the ISO if they suspect their passwords have been compromised.
- Change a provided initial password upon their first logon attempt.

All Users May

- Use media (CD, DVD, thumb drive, portable disk) provided by clients or partners for business purposes only if it is scanned for viruses before use.
- Use VDACS issued devices for occasional personal use that does not violate this or any other VDACS or DHRM policy.

All Users Must Not

- Commit any unlawful act or any act that violates current Commonwealth or VDACS policy while using a VDACS issued device.
- Take any action that jeopardizes the security of VDACS, those entities that VDACS serves, or a VDACS issued device or system. Examples of such actions include intentionally installing computer worms, viruses, or other malicious software, hacking, or using unauthorized encryption software.
- Disclose sensitive or confidential agency information or post confidential agency information to a website or other publically accessible medium
- Tamper with any security controls or attempt to bypass any security controls on a VDACS issued device for any reason.

- Install any software not approved by the agency ISO on a VDACS issued device, with the exception of mobile device users, who may download applications from the Apple iTunes store as long as these users do not violate this or any other VDACS policy.
- Modify, remove or add hardware to a VDACS issued device.
- Connect any non-VDACS computer or computing device such as personal computers, handheld devices, or printers to the COV network.
- Attempt to view, listen to, download, or store any movies, music, video, audio, or gaming entertainment from the Internet using a VDACS issued computer, except in cases where such attempts are necessary to accomplish an agency function.
- Allow anyone to use a VDACS issued device or system or share a password to any system.
    - For example, a spouse or child must not use a VDACS laptop
    - For example, a supervisor must not use an employee's account while they are out on leave.
- Auto forward agency email to an external email account
- Violate employee/client confidentiality agreements
- Intentionally abuse VDACS computing resources (destroying data or computer programs, distributing unsolicited advertising, soliciting for outside business ventures, religious or political causes, or anything that results in private or personal gain)
- Use VDACS issued devices to download, send, print, or store anything containing offensive language, sexually explicit language or pictures, or anything that is fraudulent, threatening, obscene, defamatory, intimidating, harassing, discriminatory, or otherwise unlawful.
- Use VDACS issued devices for gambling activities, except in cases where access to gambling or gaming-related sites is necessary to accomplish an agency function.
- Use non-agency email accounts to conduct agency business.
- Use shared workstations, such as those installed in a training center, to write to or modify CDs, DVDs, or thumb drives. Computer equipment not under the complete control of one employee has the potential for virus infections. Creating thumb drives and DVDs may propagate that virus. Example: Staff cannot use the shared computer in the board room to write to an external thumb drive or disc.
- Use guest, temporary, or shared accounts.
- Have multiple accounts on the same system unless authorized by the system owner, data owner, and ISO.
- Transmit any account or authentication data (e.g. passwords) electronically without the use of agency accepted encryption standards.
- Share their password with anyone, including their supervisor or any VITA personnel.
- Use a 'Remember password' feature of any application.

Remote Users

A "remote user" is any person who has been granted access to a VDACS computing resource while not physically located at a VDACS site.

Remote Users Must

- **Follow all "user" responsibilities and requirements above.**
- Obtain explicit authorization for remote access by supervisor request for a soft/hard token through the VDACS Access Request System.
- Protect information about remote access mechanisms from unauthorized use or disclosure.
- Utilize two-factor authentication to remotely connect.
- Use Virtual Private Networking (VPN) and two factor authentication to connect to the COV network via public wired or wireless (Wi-Fi) Internet or Network Access Points such as those provided in hotels, libraries, airports, client sites, or restaurants.

Remote Users May

- Use a Wireless or Wired Network if the user owns the network, as in user's home Internet or a personal wireless mobile hot spot (MiFi) device.
- Use VPN technology to access VDACS computing resources from a VDACS issued device on an approved network:
- Use a Wi-Fi Internet or Network Access Point such as those provided in hotels, libraries, airports, client sites or restaurants as long as COV VPN services are used exclusively for connection to VDACS computing resources.

Mobile Device Users

A "mobile device" is a phone (iPhone) or tablet (iPad) that (i) VDACS has assigned to a person or (ii) is a personal phone that accesses the COV network for business use.

A "mobile device user" is any person who (i) has been assigned a VDACS mobile device or (ii) uses a personal phone for business use. A person who uses a personal phone for business use shall only be considered a mobile device user when such personal phone accesses the COV network.

Mobile Device Users Must

- **Follow all "user" responsibilities and requirements above.**
- Register the mobile device with the Telecommunications Coordinator.
- Mark a VDACS issued mobile device to clearly identify it as a Commonwealth device and indicate a method of return if the device is lost.
- Understand that the mobile device is configured to:

- receive security policy and configuration information from COV Mobile Policy Servers
- Engage a screen lock after a maximum of 15 minutes of inactivity
- prohibit the storage of passwords in clear text
- automatically wipe the contents of a VDACS issued device if 10 consecutive invalid logon attempts
- use a password of no less than 4 characters
- not reuse a password prior to 24 password changes
- not cache passwords on the device
- suppress the display of passwords on the screen as the password is entered into the device
- use an encrypted network at all times when accessing the COV network
- only use the boot ROM and operating system as supplied by the device vendor/carrier
- not allow the user to escalate the base privilege level

- Install all security updates within 30 days of release by the original equipment manufacturer or authorized device reseller.
- Acknowledge that VDACS personnel or Commonwealth Security personnel may seize the device any time for investigation, or wiped without warning and for any reason.

Mobile Device Users May

- Use a Wireless or Wired Network under the conditions outlined in the Remote User section, or use the device mobile connection.
- Use a public Wi-Fi Internet or Network Access Point such as those provided in hotels, libraries, airports, client sites or restaurants as long as COV VPN services or Enterprise Handheld Services (EHS) AirWatch are used exclusively for connection to COV data and resources.
- Connect the COV mobile device to a VDACS issued computing device for Sync, data transfer, or charging.
- Download applications from the Apple iTunes store as long as they do not violate this policy.
- Review the mobile device process document located at https://lap01152.cov.virginia.gov:8890/intranet/facilities.htm
- Be reimbursed for the use of a personal phone for business use under the following conditions:
  - Approved devices that are provisioned to support voice and data or data-only functions (i.e. smart devices).
  - Be authorized a single stipend for the use of a single personal phone for business use. Exceptions to this may be granted by the agency head.
  - The maximum allowed reimbursement is $45 per month. VDACS reserves the right to change the maximum allowed reimbursement

at any time in order to comply with changes to external governing bodies.
    - Signs a "VDACS Mobile Device Allowance Agreement "and has approval of, the employee's supervisor and agency or designee.

Mobile Device Users Must Not

- Share the device with any family members or other parties not specifically authorized.
- Use a mobile device while driving a state vehicle; except in cases of emergency, during which times the mobile device may only be used for voice communication.
- Text message at any time while driving any vehicle
- Leave the VDACS mobile device in an unattended personal or state vehicle unless it is securely locked and not visible.
- Connect the VDACS mobile device to a personal or other non-VDACS provided computer for any reason.
- Take the VDACS mobile device out of the continental United States for any reason. A loaner device can be provided for international travel but upon return the following steps must be taken:
    - Do not connect the VDACS issued phone or tablet to a COV network until that VDACS issued phone or tablet has been examined and wiped clean/erased by technology staff.
- Make "Operator Assisted" calls or other charged activities such as 411 directory services without a valid business need.
- Use a VDACS credit card to make iTunes media or application purchases unless they are approved through standard procurement practices.

Supervisors and Managers

A "supervisor" or "manager" is any person who has been assigned the responsibility of managing other personnel, contractors, or vendors.

Note: Where it is shown that supervisors or managers were aware of a user playing a part in an ongoing security violation, demonstrating a disregard for safe computing practices through repeated security incidents, or failing to complete assigned training, the supervisor or manager will also be subject to disciplinary action.

Supervisors and Managers Must

- **Follow all "user" responsibilities and requirements above.**
- Ensure any users reporting to the supervisor or manager:
    - Follow all security policies, procedures, and guidelines;
    - Complete annual security awareness training requirements;
    - Report any security incidents in a timely manner.

- Report any user status change that could affect security such as:
  - Suspensions
  - Transfers
  - Terminations
- Report any security incident that users may become aware of to the ISO immediately.
- Verify that employees have read this policy and agree with the non-disclosure clauses during the performance evaluation process.
- Use the agency Access Request System for access for employees to create a new account, make modifications to an existing account, terminate an existing account, or disable an existing account. Terminations must be submitted immediately upon an employee's separation from VDACS.
- Authorize and approve all account access actions (new, change, or termination).
- Request temporary disabling of physical and logical access rights through the Access Request System when personnel are not working for a prolonged period in excess of 30 days due to leave, disability, or other authorized purpose. Exceptions may be submitted by an employee's supervisor to the Director of Human Resources, who will notify the agency ISO. The request must include justification for the request and the length of time requested.
- Request the temporary disable of physical and logical access rights through the Access Request System upon suspension of an employee for greater than one (1) day for disciplinary purposes. The request must be submitted through the VDACS Access Request System.
- Request the disabling of accounts of a user posing a significant risk to information systems. The request to disable must be entered into the VDACS Access Request System or the VDACS ISO must be notified within four hours of the discovery of the risk situation. The ISO can be reached via email at Deborah.nickerson@vdacs.virginia.gov, or at 804-786-0489, 804-921-6786, or 804-874-6242.
- Must establish separation of duties in order to protect sensitive data on a VDACS computing resource or establish compensating controls when constraints or limitations of the agency prohibit a complete separation of duties. Such compensating controls may include increased supervisory review, reduced span of control, rotation of assignments, independent review, monitoring and/or auditing, and times and specific access authorization with audit review.

Supervisors and Managers May

- Request assistance from the ISO if users would like specific or general security requirements explained to users.

Supervisors and Managers Must Not

- Allow any user to violate VDACS or Commonwealth security policies or procedures.

System Owners

A "system owner" is any agency business manager responsible for operating or maintaining an IT system.

System Owners Must

- **Follow all "user" responsibilities and requirements above.**
- Require that the IT system users complete any system unique security training prior to, or as soon as practicable after, receiving access to the system, and no less than annually, thereafter.
- Manage system risk by adhering to any additional information security policies and procedures required to protect the system in a manner commensurate with risk.
- Maintain compliance with VDACS Information Security policies and standards in all IT system activities.
- Maintain compliance with requirements specified by data owners for the handling of data processed by the system.
- Authorize whether or not a system is eligible for remote access
- Designate two system administrators for the system.
- Investigate any unusual IT system access activities and take appropriate action when needed.
- Establish separation of duties in order to protect sensitive data on a VDACS computing system, or establish compensating controls when constraints or limitations of the agency prohibit a complete separation of duties. Such compensating controls may include increased supervisory review, reduced span of control, rotation of assignments, independent review, monitoring and/or auditing, and times and specific access authorization with audit review.

Data Owners

A "data owner" is any agency manager responsible for the policy and practice decisions regarding data.

Data Owners Must

- **Follow all "user" responsibilities and requirements above.**
- Evaluate and classify sensitivity of the data they manage
- Define protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs.
- Communicate data protection requirements to the system owner.
- Define requirements for access to the data.
- Investigate any unusual IT system access activities and take appropriate action when needed.
- Establish separation of duties in order to protect sensitive data on a VDACS computing system, or establish compensating controls when

constraints or limitations of the agency prohibit a complete separation of duties. Such compensating controls may include increased supervisory review, reduced span of control, rotation of assignments, independent review, monitoring and/or auditing, and times and specific access authorization with audit review.

System Administrators

A "systems administrator" is any employee or contractor who implements, manages, and/or operates a system or systems at the direction of the system owner or data owner.

System Administrators Must

- **Follow all "user" responsibilities and requirements above.**
- Assist agency management in the day-to-day administration of agency IT systems.
- Implement security controls and other requirements of the agency information security program on IT systems for which they have been assigned responsibility.
- Have a second account specifically for the purpose of system administration if the user is designated as a system administrator. Administrators are required to use their administrative account only when performing tasks required as a system administrator.

Information Systems Staff

An "information systems staff" is any person assigned to Administrative and Financial Services, Information Systems office who provides technology support to other agency employees.

Information Systems Staff Must

- **Follow all "user" responsibilities and requirements above.**
- Provide system owners an annual review of all user accounts for sensitive IT systems to assess the continued need for the accounts and the access level and periodic review of user accounts for other IT systems.
- Provide system owners an annual review of all shared/group accounts for review. Shared/group accounts are items such as distribution lists, security groups, or other group membership accounts.
- Ensure passwords displayed on a screen are suppressed as they are entered.
- Ensure access to any files containing passwords is limited to the file owner, the application/system, or the technical system administrator.
- Develop and interpret information security policies and procedures to comply with overall intent of the COV standards that are meaningful and obtainable considering agency goals and resources.

- Assist System Owners by developing additional policies and procedures commensurate with risk.

Information Systems Staff Must Not

- Include passwords in plain text in scripts.

VIOLATIONS

Any infractions of this agreement may result in disciplinary action, including, but not limited to, the termination of access privileges.

Report alleged violations of this policy to the Director of Information Systems and the ISO. The Director of Information Systems or the ISO must refer alleged violations of this policy to the Director of Administrative and Financial Services and the Director of Human Resources. Upon completion of a review of the allegations, a report will be provided to the VDACS Deputy Commissioner. The VDACS Commissioner, on the recommendation of the Human Resource Office and the VDACS Deputy Commissioner, may refer alleged violations of state or federal law to the appropriate law enforcement officials.

AUTHORITY AND INTERPRETATION

The Commissioner of Agriculture and Consumer Services issues this policy pursuant to authority granted under the laws and regulations of the Commonwealth of Virginia.

The Director of Administrative and Financial Services is responsible for official interpretation of this policy as it relates to procurement, operation, and maintenance of agency information technology. The Director of Human Resources is responsible for official interpretation of this policy as it relates to employee performance and related issues that may be handled under DHRM Policy 1.60, Standards of Conduct.

RELATED POLICIES AND PROCEDURES

- Department of Human Resource Management (DHRM) Policy 1.75, Use of Electronic Communications and Social Media
- Virginia Information Technology Agency Information Security Standard COV SEC 501 (incorporated into VDACS policy 10.1)
- VDACS 10.3 Business Use of Social Media