Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6515
Transmittal Sheet
June 28, 2011

USE OF WEB-BASED COLLABORATION TECHNOLOGIES

1. REASON FOR ISSUE: The Department of Veterans Affairs (VA) endorses the secure use of Web-based collaboration and social media tools to enhance communication, stakeholder outreach collaboration, and information exchange; streamline processes; and foster productivity improvements. Use of these tools supports VA and VA's goal of achieving an interoperable, net-centric environment by improving employee effectiveness through seamless access to information. Web-based collaboration tools enable widely dispersed facilities and VA personnel to more effectively collaborate and share information—which can result in better productivity, higher efficiency, and foster innovation. This Directive establishes policy on the proper use of these tools, consistent with applicable laws, regulations, and policies.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This Directive provides mandatory instruction for all VA offices and employees regarding the use of emerging Web tools to facilitate collaboration and information sharing at VA.

3. RESPONSIBLE OFFICE: Office of the Assistant Secretary for Information and Technology (005), Office of the Assistant Secretary for Public and Intergovernmental Affairs (002); in collaboration with Office of Information Protection and Risk Management (005R), Associate Deputy Assistant Secretary (ADAS), Office of Privacy and Records Management (005R1), Director of Online Communications (002).

4. RELATED HANDBOOK: None.

5. RESCISSION: None.

CERTIFIED BY:

/s/

Roger W. Baker
Assistant Secretary for
Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/

L. Tammy Duckworth
Assistant Secretary for
Public and Intergovernmental Affairs

Distribution: Electronic Only

USE OF WEB-BASED COLLABORATION TECHNOLOGIES

1. PURPOSE

a. This Directive provides policy for all Department of Veterans Affairs (VA) offices and employees regarding the use of Web-based resources and tools to facilitate collaboration, outreach, communication, and information sharing at VA. These web-based collaborative tools include social media such as wikis, blogs, mashups, folksonomies, Web feeds (such as Really Simple Syndication (RSS) feeds), and forums (such as Facebook, chat rooms), and collaborative tools such as Microsoft SharePoint. Properly used, these tools can significantly enhance VA's mission effectiveness.

b. Benefits of Web-based collaboration and social media technologies include:

(1) Speed – quick dissemination of information;

(2) Broad reach – vast networks and super-networks of technology and users;

(3) Targeted reach – a growing number of interest groups represent topics of specific interest to Veterans, Servicemembers, and their families; VA employees; volunteers; trainees; contractors or other appointees;

(4) Collaboration – both organizations and the public use Web-based tools to network, build relationships, and look for mutually beneficial collaboration opportunities;

(5) A medium for dialogue – developers often have the access needed to create new applications and to better assess, measure, and use the technology; and

(6) Expansion of real-time, sensitive communications – helpful for communication during a disaster or emergency situation.

c. This policy applies to the use of Web-based collaboration tools on any VA Internet/Intranet domains or servers as well as any Federal or commercial site in which individuals represent the Department. The policy applies to all individuals designing, contributing, maintaining, using, or providing oversight of these tools. Individuals include but are not limited to, full-time and part-time employees, contractors, interns, and volunteers who access or contribute content.

2. POLICY

a. The use of Web-based collaboration tools such as social media tools is *highly* encouraged. Web-based collaboration is intended for information sharing within and outside of VA. To increase accountability, promote informed participation by the public, and create economic opportunity, the presumption shall be in favor of openness (to the extent permitted by law and subject to the exclusions noted in this Directive or other policy)

b. VA endorses the secure use of Web-based collaboration tools to enhance communication, collaboration, information exchange, and citizen engagement; streamline processes; and foster productivity improvements, when it is done in accordance with applicable laws, regulations, and policies. Web-based collaboration tools enable widely dispersed facilities and VA staffs to more effectively collaborate and share information to achieve greater productivity, efficiency, and innovation.

c. VA entities will promote accessibility of collaboration tools. Where access to social media sites may intrude upon business operations, local leadership may deem it necessary to limit or block access to social media sites for that organization. Leadership will notify the appropriate administration's or staff office's designated office for Web oversight, the Assistant Secretary for Information and Technology, and the Assistant Secretary for Public and Intergovernmental Affairs and provide justification for the denial.

d. VA personnel and organizations must exercise sound judgment when utilizing Web-based collaboration tools. The use of VA Web-based collaboration tools must promote the mission, goals, and objectives of VA. Such use must also be consistent with applicable laws, regulations, and policy, as well as prudent operational, security, and privacy considerations.

e. VA personnel and organizations engaged with these technologies are responsible for ensuring that their use complies with applicable laws, regulations, and policies, including guidance from the Office of Management and Budget, and VA Directives and Handbooks 6102, Internet and Intranet Services and 6500, Information Security Program.

f. VA personnel must maximize the quality, objectivity, utility, and integrity of information and services provided to the public. As such, when officially representing the Department, VA personnel must reasonably ensure that the agency position on a topic is properly represented in all communications. Articles and features about VA programs or initiatives that are intended for public release must follow VA policy.

g. Web-based collaboration tools established for official VA use must be authorized, monitored, and moderated. As the content owners, each administration, staff office, program office, and facility is responsible for monitoring and maintaining all posted Web content and assuring that the information is accurate and current. Additional policy and guidance is available in VA Directive and Handbook 6102.

h. To establish an official VA social media account, the petitioning office/employee/organization must demonstrate 1) a business case for the site, 2) that adequate resources are available to establish and maintain the site, and 3) that the organization's previously established website is also kept up-to-date and meets VA quality standards. The Office of Public and Intergovernmental Affairs (OPIA) is the final approving authority for all VA social media sites, except those of the Office of the Inspector General,

which is exempt from this oversight and control per the Inspector General Act, 5 U.S.C. App. 3. However, OPIA may delegate approval or disapproval to administration communications offices after coordinating with those offices to ensure the maintenance of content standards.

i. When a VA-owned or VA-managed collaborative workspace or social media tool is used to retrieve records pertaining to individuals by their name or other personal identifier, a system of records notice will be required and other protections will apply in accordance with the Privacy Act.

j. A Web Page Privacy Policy (or link to the approved statement) must also be posted on the introductory page in accordance with VA Handbook 6502.3, .

k. VA personnel represent a rich source of information for Veterans. As such, VA employees are encouraged to interact with the public online as long as that interaction does not interfere with the employee's performance of his or her official duties. However, such activity comes with responsibility. When interacting with the public online, VA employees must draw a clear distinction between their personal views and their professional duties. Employees who are not officially authorized to speak on behalf of VA must never state or infer their communications represent VA's official position. Similarly, employees should discourage Veterans and associated participants from seeking official VA determinations or adjudications via social media. In these cases, employees must be clear that these requests must be submitted through the designated official channels to ensure proper protection of personal information and for an official response to be provided.

l. Social media websites must not be used to monitor an individual's exercise of his or her First Amendment rights unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to, and within the scope of, an authorized law enforcement activity. Under certain circumstances, leadership may elect to publicly respond to or participate in these electronic fora.

m. VA employees must edit submissions by the public that contain vulgar language, personal attacks of any kind, or offensive comments that target or disparage any individual or group. Further, VA employees will delete comments that:

(1) Are spam;

(2) Are clearly off topic;

(3) Advocate illegal activity;

(4) Promote particular services, products, or political organizations;

(5) Infringe on copyrights or trademarks;

(6) Contain unauthorized release of VA Sensitive Data; or

(7) Clearly violate VA Privacy Policy.

n. When it becomes necessary to officially contact individuals, VA employees generally shall not use social media outlets as an official mechanism for contacting individuals. In order to ensure continuity of access to all externally hosted, VA-sponsored Web-based social media tools, any account used by VA parties to disseminate official VA information shall be established using a VA group email address. Personal or individual VA email addresses will not be used to the extent practicable as a result of unique and varied social media and Web-based collaboration tool platforms' terms of service.

o. All VA social media pages or sites must contain the "Social Networking Disclaimer" found in Appendix A. If the notice is not on the main page, the homepage must include a prominent link to the notice. In these cases, the marking must clearly identify the notice as "Privacy and Security - Legal Notice."

p. VA pages or sites must alert the visitor of any link that leads to a third-party website or any other location that is not part of an official government domain, through a statement adjacent to the link or a pop-up, that explains that the visitor is being directed to a nongovernment Website and that the Website may have privacy policies that differ from VA.

q. VA-hosted Web-based collaboration tools must comply with Section 508 of the Rehabilitation Act of 1973. Where the dissemination of information in accordance with the Accessibility Standards constitutes an undue burden on the agency, a non-accessible non-Federal website may still be used, but VA personnel must make the information available in alternative formats.

r. While automated collaborative tools present many useful opportunities, their use must not compromise data confidentiality and integrity. The Intranet provides a secure environment to operate most Web-based collaboration tools; however, the Internet exposes VA information systems to external threats that could adversely impact operations, potentially threatening data confidentiality, integrity, and availability. Therefore, precautions must be taken when planning to implement Web-based collaboration technologies or integrating these tools into the VA environment.

s. VA personnel and organizations are responsible for the secure use of Web-based collaboration tools with respect to sensitive information. Each office or facility has responsibility for evaluating the sensitivity of the data to be used, and to ensure the monitoring and maintenance Web content with respect to any sensitivity issues. VA personnel are responsible for accessing, using, and disseminating content in accordance with legal authorities governing sensitive information.

t. Access to Web-based collaboration tools that access, disseminate, or process sensitive information must be restricted to those VA personnel who have a need to know for the performance of their professional duties. Data must be properly safeguarded in accordance with VA Directive and Handbook 6500, and any applicable laws and regulations. Any actual or suspected breach of sensitive information must be reported to his or her supervisor and the Privacy Officer or the Information Security Officer within one hour of discovery in accordance with VA Handbook 6500.2., Management of Security and Privacy Incidents and VA Handbook 6502.1, Privacy Event Tracking. This policy applies to any VA data hosted entries on VA or commercially-hosted sites.

u. The Privacy Act, the HIPAA Privacy Rule, and other privacy statutes and regulations may apply to certain information for which Web-based collaboration tools are used. Content owners must consult with the Privacy Officer of the facility or agency component to ensure that they comply with all legal requirements for protected information.

v. All possible steps must be taken to ensure confidentiality, integrity, and availability of information. These steps include, but are not limited to, system redundancy, automated electronic backups, and secure data storage as well as proper and timely data disposal and media sanitization.

w. VA Web-based collaboration tools made publicly available are required, to the extent practicable and necessary to achieve their intended purposes, to provide all data in an open industry standard format that permits users to aggregate, disaggregate, or otherwise manipulate and analyze the data in order to meet their needs.

x. Any Web-based collaborative tool which involves data capture of PII may require a System of Record Notice (SORN) and a Privacy Act Statement under the Privacy Act and the Paperwork Reduction Act. The Privacy Act Statement must describe the legal authority for the collection of the information, the purpose for the collection of the data, how the information may be shared outside of VA (routine uses), and whether the provision of the information is mandatory or voluntary under law. Web-based collaboration tools must also meet standard records retention and e-discovery requirements as mandated by law.

y. The use of Web-based collaboration tools for research/collaboration must adhere to applicable VA regulations and policies and guidance as determined by the respective Administration or Staff Office. As determined by each respective Administration, Staff Office, additional policies covering proper collection, use, dissemination, management, and destruction of the information may be published in collaboration with the appropriate VA offices responsible for privacy, security, and information technology.

3. RESPONSIBILITIES

a. **The Secretary of Veterans Affairs.** The Secretary has designated the Department's Assistant Secretary for Information and Technology (AS/IT) as the Department's CIO, the senior agency official responsible for the Department's IT programs.

b. **The Assistant Secretary for Information and Technology.** As the CIO, the AS/IT is responsible for the effective use of VA's Internet, Intranet and other IT resources, and for agency-wide directives, and policies governing the use and implementation of Internet/Intranet and other IT resources. The AS/IT shall:

(1) In conjunction with the AS/OPIA, publish policy and procedural guidance for the usage or establishment, operation, and maintenance of Web-based collaboration tools, including websites operated by non-VA entities;

(2) Ensure that secure access is provided to all approved Web-based collaboration tools

(3) In conjunction with the AS/OPIA, establish Department-wide requirements, and provide oversight and guidance related to Web-based collaboration tools;

(4) Designate the Deputy Assistant Secretary, Information Security (DAS/IS), as the principal Department official responsible for ensuring Department-wide compliance with Federal guidance on the use of Web-based collaboration tools;

(5) Approve the Director, VA Privacy Service as the official responsible for the handling of privacy matters as they relate to Web-based collaboration tools;

(6) Work with the Assistant Secretary for Public and Intergovernmental Affairs (AS/OPIA) to develop a Web-based collaboration strategy that addresses the guidelines set forth within this policy and by Federal guidance on the use of social media; ensure the AS/OPIA is notified when access to social media sites is blocked at VA facilities; and

(7) Work with the Assistant Secretary of Human Resources and Administration to develop and establish standard operating procedures for disabling access for individuals who establish, maintain, or are responsible for posting content to externally-hosted Web-based collaboration tools when those individuals transfer or are terminated from these duties.

c. **The Deputy Assistant Secretary for Information Security. The DAS/IS** shall:

(1) Issue information protection policy in accordance with this Directive;

(2) Ensure that a risk assessment has been conducted, including consideration of the level of assurance and appropriate authentication requirements for outsourced systems or services, in accordance with applicable Federal laws and standards for system authorization, certification, and accreditation;

(3) Review configuration and implementation plans for production hardware and software solutions to ensure the social media provider maintains an appropriate configuration, patch, and technology refresh level;

(4) Work with the DAS for Enterprise Development and the DAS for Enterprise Operations and Infrastructure to explore standardizing the desktop image to secure the Internet connection through a Trusted Internet Connection (TIC); and

(5) Provide specialized training to educate users of Web-based collaboration tools about what information to share, with whom they can share it, and what must not be shared.

d. **Director, VA Privacy Service.** The Director, VA Privacy Service shall:

(1) Work with Web-based collaboration service coordinators, General Counsel (GC), and AS/OPIA to ensure that all privacy matters are addressed with regard to the use of Web-based collaboration tools; and

(2) Determine whether waivers will be provided to Program Offices and facility sites whose PII has not been accessed for more than 90 days, and grant or deny such waivers and work with the ADAS for Cyber Security to identify systems that have not been granted waivers in order to ensure that any PII is properly disposed.

e. **Assistant Secretary for Public and Intergovernmental Affairs (AS/OPIA).** The AS/OPIA manages communications with Veterans, the general public, VA employees, and the news media. This responsibility includes coordination and distribution of the information VA communicates to its audiences, especially to the general public through the news media, and the provision of public affairs policy guidance for the Department. The AS/OPIA shall:

(1) Work with Web-based collaboration service coordinators, GC and the ADAS for Privacy and Records Management to ensure that all public affairs concerns are addressed regarding the use of Web-based collaboration tools ;

(2) Provide guidance on acceptable content for Web-based collaboration tools;

(3) Work with the AS/IT to develop a Web-based collaboration strategy that addresses the guidelines set forth within this policy adheres to Federal guidelines on the use of social media;

(4) Review and approve or disapprove requests by VA organizations to launch official social media presences;

(5) Have the authority to disapprove any outward-facing content on official VA blogs and social media sites which do not meet accepted standards of quality;

(6) Designate the Director of Online Communications, Office of Public Affairs, as the official responsible for providing organizations throughout the Department content standards for the use of online communications;

(7) Conduct periodic review of social media sites to ensure alignment with Department messaging and priorities and certify that those sites may continue to operate after audits are concluded; and

(8) Work with the appropriate VA Records Officer and the National Archives and Records Administration (NARA) to establish a Records Control Schedule (RCS) for VA records generated via VA social media that are not covered by an existing RCS.

f. **General Counsel (GC).** GC shall:

(1) Provide legal reviews, as appropriate, for agreements with Web-based social networking services;

(2) Work with Web-based collaboration service coordinators, OPIA, and the ADAS for Privacy and Records Management to ensure that all legal concerns are addressed regarding the use of Web-based collaboration technologies; and

(3) Provide legal reviews of content involving mission-related legal matters.

g. **Assistant Secretary for Operations Security and Preparedness (AS/OSP).** The AS/OSP shall provide guidance to Web-based collaboration service coordinators establishing communications, roles, and responsibilities for handling threats received from members of the public via Web-based collaboration tools.

h. **Under Secretaries, Assistant Secretaries, and Other Key Officials.** These officials shall:

(1) Ensure that VA information and information resources are protected from unlawful and unauthorized use, access, tampering, destruction, and unauthorized release of VA sensitive information;

(2) Ensure that Web-based collaboration tools that are made publicly available are required, to the extent practicable and necessary to achieve their intended purposes, to provide all data in an open industry standard format that permits users to aggregate, disaggregate, or otherwise manipulate and analyze the data in order to meet their needs;

(3) Ensure that access to approved Web-based collaboration tools are provided to those VA employees who have a need for it in order to perform work-related tasks and to those who maintains or provides official VA content for said tools;

(4) Provide proper records management retention in accordance with the applicable Freedom of Information Act (FOIA) requirements, e-discovery litigation holds, and RCS, or if the records are unscheduled under an RCS, ensure that they are retained until they are scheduled by the Archivist of the United States;

(5) Ensure that mechanisms are in place, prior to permitting the use of Web-based collaboration tools, to remind users of VA policy and of their obligations to protect VA sensitive data;

(6) Monitor and maintain all Web content posted in support of programs and initiatives under their control;

(7) Ensure that all externally-hosted social networking sites have a corresponding site located behind the VA firewall as the official source for information pertaining to the subject presented on the externally-hosted website; and

(8) Issue policies in support of this Directive.

i. **DAS for Enterprise Development and DAS for Enterprise Operations and Infrastructure.** These officials shall work with the DAS for Enterprise Development and the DAS for Enterprise Operations and Infrastructure to explore standardizing the desktop image to secure the Internet connection through a TIC.

j. **VA CIO Office of Enterprise Development, Resource Management Information Technology ((OED RMIT) (005Q)).** OED RMIT shall support and manage VA's Web-based collaboration presence and ensure compliance with all Federal mandates and guidance, and in accordance with Department-wide policies, initiatives and requirements thereof.

k. **Associate Deputy Assistant Secretary (ADAS) for Cyber Security.** ADAS for Cyber Security shall work with the Director.

l. **Program Offices and Facility Sites.** The Web Communications Office for each administration or staff office is responsible for the following tasks, but may delegate to program and field office heads the responsibility to:

(1) Ensure the content of the documents posted on the website (including papers, studies, forms, pictures, and graphics) is current, accurate, factual, relevant to the VA mission, and spell-checked and grammatically correct;

(2) Ensure that VA Internet and intranet services and websites operating on VA's behalf conform to Section 508 of the Rehabilitation Act of 1973, as amended;

(3) Attain a waiver from the VA Privacy Service if there is a need to retain PII that has not been accessed for more than 90 days;

(4) Ensure that Internet and intranet website server environments under his/her purview are secured as outlined in VA policy and coordinate with their ISOs about any security issues that are material to an environment that falls within the purview of OI&T.

(5) Ensure that all externally-hosted social networking websites for programs under their control have a corresponding website located behind the VA firewall that is used as the official source for information pertaining to the subject presented on the externally-hosted website; and

(6) Designate a Web Content Manager (as defined in VA Directive 6102 *Internet/Intranet Services*) to be accountable for any information dissemination on any official externally-facing VA internet sites which represent their respective organizational mission. (Note: While it is preferred that different people serve as Web-based collaboration service coordinators and content manager(s), these roles may be combined if appropriate.)

m. **Web-based Collaboration Service Coordinators.** Web-based collaboration service coordinators must:

(1) Consider the data protection aspects of their activity, and in particular, whether it involves the transfer of VA sensitive information outside of VA;

(2) Only use a technology which requires users to submit personal data if such use is optional. Where a Web-based collaboration service requires the transfer of PII (e.g., for account set-up), this transfer must be left to each user to accomplish;

(3) Use settings that allow for distinction between official VA postings and publicly-created content when they are available. Such settings should also:

(a) Allow VA-created content to be clearly delineated from that provided by the public;

(b) Be optimized for VA's needs to communicate, distribute information and content, engage the public, and capture new audiences through viral marketing. An example of this is the use of a Facebook "page" that will only allow for fans, as opposed to a Facebook "profile" that will allow for friends;

(4) Follow the VA procedures for authorizing transfers of PII and other confidential information to suppliers and contractors including:

(a) Consulting with his or her ISO and PO when proposing to transfer PII to an external service;

(b) Undertaking a PIA to identify potential risks and liabilities and actions necessary to mitigate these risks; and

(c) Ensuring that all suppliers and contractors processing PII or other confidential information on behalf of VA sign VA confidentiality agreement before the data is transferred;

(5) Ensure that all social media websites for which they are responsible remain on topic and do not contain:

(a) PII

(b) Excessive vulgar language

(c) Personal attacks of any kind

(d) Offensive comments that target or disparage any protected class

(e) Spam

(f) Subjects clearly off topic

(g) Language advocating illegal activity

(h) Promotions of particular services, products, or political organizations

(i) Copyrights or trademarks not owned by the person posting them

(j) Contain VA sensitive data or

(k) Clearly violates the VA policy

(6) Ensure that all links remain current or discontinued when linked content is no longer available;

(7) Review all blogs and other relevant content regularly as prescribed by the Office of Public Affairs and/or Director of Online Communications. Blogs and other social media sites remaining idle for 30 days may be removed at the discretion of the Office of Public Affairs unless those idle periods are coordinated in advance;

(8) Answer questions posted to blogs and other social media sites by the public within a reasonable period of time and/or as prescribed by the Office of Public Affairs and/or Director of Online Communications;

(9) Ensure that all information posted through the use of Web-based collaboration tools will be in accordance with VA Directive 6361, Ensuring Quality of Information Disseminated by VA;

(10) Inform and receive clearance from OPIA before launching any public-facing website that involves the use of Web-based collaboration tools;

(11) Ensure that VA Internet and intranet services and websites operating on VA's behalf conform to Section 508 of the Rehabilitation Act of 1973, as amended; and

(12) Ensure that all VA blogs under their responsibility contain the "Social Networking Disclaimer" found in Appendix A.

n. **VA Records Officer.** VA Records Officer shall:

(1) Work with content owners to ensure that all records generated through the use of Web-based collaboration tools adhere and conform to all documentation contained in the applicable RCS; and

(2) Work with the Archivist of the United States and VA content owners to determine the most appropriate method(s) to capture and retain VA records on both Federal servers and VA activities hosted on non-Federal Web-based collaboration hosts.

o. **Information Security Officers**. Information Security Officers shall:

(1) Work with content owners to ensure that all information security program policies, procedures, and practices, as they apply to the particular use of Web-based collaboration tools are addressed;

(2) Serve as advisors on all aspects of information security to their Administrations or program areas; and

(3) Monitor and assist in the administration of VA information security training and or awareness programs with their responsibility and as it applies to the particular use of Web-based collaboration tools.

p. **VA Personnel.** VA personnel utilizing Web-based collaboration technologies:

(1) Wherever possible, these individuals must use the VA intranet for the conduct of VA business. VA personnel using external technologies for collaboration activities must ensure that this use complies with law, guidance, and VA policy;

(2) When acting in or outside of their official capacities, VA personnel must remember that they are personally responsible for the content they publish on blogs, wikis or any other form of user-generated media, and be mindful that what is published will be public for a long time; (in some cases, a personal disclaimer should be written to indicate that the speaker is not representing the VA or their respective program).

(3) When interacting on weblogs (blogs), wikis, social networks, virtual worlds and social media, VA Personnel must:

(a) Never comment on VA mission-related legal matters unless they are VA's official spokesperson for the matter, and have GC and management approval to do so;

(b) Be professional at all times when posting to VA-related social media, and use their best judgment when interacting on social media about matters related to VA's mission;

(c) In their capacities as VA representatives, post only information about which they have actual knowledge. They must never comment or provide information on any matter about which they do not have actual, up-to-date knowledge;

(d) Identify themselves and their roles as VA representatives when commenting or providing information on matters related to the VA mission;

(e) Be aware of their associations with VA in online social networks. If they identify themselves as VA representatives, ensure that their profiles and any related content is consistent with how they wish to present themselves to colleagues, members of the Executive and Legislative Branches of the Federal government, and the general public;

(f) Never post information protected by the Health Insurance Portability and Accountability Act (HIPAA), The Privacy Act of 1974, 38 USC 5701, 5705, or 7332, or VA policy on any Web-based collaboration tool without legal authority and prior approval by authorized official, and unless proper, VA approved security measures are in place. All employees, contractors and other persons will have access as appropriate to the performance of their official VA duties;

(g) Never use profanity, make libelous statements, or use privately-created works without the express, written permission of the author. Never quote more than short excerpts of other people's work;

(h) Only post and use content in accordance with applicable ethics, intellectual property, records, and privacy laws, regulations, and policies;

(i) Use Government Office Equipment including IT in accordance with VA Directive 6001, *Limited Personal use of Government Office Equipment Including Information Technology* and;

(j) Use only instant messaging services approved by VA.

4. REFERENCES.

a. E-Government Act of 2002, Pub. L. 107-347, Section 208.

b. 36 C.F.R. Part 1236, Electronic Records Management.

c. Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules.

d. Fraud and Related Activity in Connection with Access Devices and Computers, 18 U.S.C. 1029-1030.

e. Freedom of Information Act (FOIA), 5 U.S.C. 552, 38 C.F.R. §§ 1.550-557.

f. Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. 104-191.

g. Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, 45 C.F.R. Parts 160 and 164.

h. National Institute for Standards and Technology Special Publication 800-24, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2004.

i. National Institute for Standards and Technology Special Publication 800-44, Guidelines on Securing Public Web Servers, September 2007.

j. National Institute for Standards and Technology Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations, August 2009.

k. National Institute for Standards and Technology Special Publication 800-61, Computer Security Incident Handling Guide, December 1998.

l. National Institute for Standards and Technology Special Publication 800-63, Electronic Authentication Guideline 800-63, April 2006.

m. National Institute for Standards and Technology Special Publication 800-83, Guide to Malware Incident Prevention and Handling, November 2005.

n. National Institute for Standards and Technology Special Publication 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, September 2006.

o. National Institute for Standards and Technology Special Publication 800-95, Guide to Secure Web Services, August 2007.

p. OMB Circular A-130, Management of Federal Information Resources, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals, November 28, 2000.

q. OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Systems, March 02, 2006.

r. OMB M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003.

s. OMB M-04-07, Social Media, Web-based Technologies, and the Paperwork Reduction Act, April 7, 2010.

t. Privacy Act of 1974, 5 U.S.C. 552a, 38 CFR §§ 1.575 – 1.584.

u. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. 107-56, Title II.

w. VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology.

x. VA Directive 6102, Internet and Intranet Services.

y. VA Directive 6221, Accessible Electronic Information Technology (EIT).

z. VA Directive 6300, Records and Information Management.

aa. VA Directive 6361, Ensuring Quality of Information Disseminated by VA.

bb. VA Directive 6371, Destruction of Temporary Paper Records.

cc. VA Directive 6500, Information Security Program.

dd. VA Directive 6502, VA Enterprise Privacy Program.

ee. VA Directive 6507, Reducing the Use of Social Security Numbers.

ff. VA Directive 6508, Privacy Impact Assessments.

gg. VA Directive 6600, Responsibility of Employees and Others Supporting VA in Protecting Personally-Identifiable Information (PII).

hh. VA Directive 6609, Mailing of Sensitive Personal Information.

ii. VA Handbook 6310.2, Collections of Information Procedures.

jj. VA Handbook 6361, Ensuring Quality of Information Disseminated by VA.

kk. VA Handbook 6502.3, Web Page Privacy Policy.

ll. 38 U.S.C. 5701, Confidential Nature of Claims, 38 C.F.R. 1.500-527.

mm. 38 U.S.C. 5705, Confidentiality of Medical Assurance Records, 37 C.F.R. 17.500-511.

nn. 38 U.S.C. 5721-5727, Information Security, 38 C.F.R. 75.111-118.

oo. 38 U.S.C. 7332, Confidentiality of Certain Medical Records, 38 C.F.R. 1.460-496.

5. DEFINITIONS

a. **Accreditation.** The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls

b. **Certification.** A comprehensive assessment of the management, operational and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

c. **Folksonomy.** The term folksonomy means a system of classification derived from the practice and method of collaboratively creating and managing tags to annotate and categorize content. This practice is also known as collaborative tagging, social classification, social indexing, and social tagging.

d. **Government Office Equipment Including Information Technology.** Government office equipment including IT, encompasses, but is not limited to: personal computers and related peripheral equipment and software, library resources, telephones, facsimile machines, photocopiers, office supplies, Internet connectivity, and access to Internet services and E-mail. This list is provided to show examples of office equipment as envisioned by this policy.

e. **Individual.** The term individual includes employees of VA, properly appointed volunteers, VA contractors, VA beneficiaries and their dependents or survivors, and others with whom VA has a business relationship and collects or stores social security numbers.

f. **Mashup.** A mashup is a Web page or application that uses and combines data, presentation or functionality from two or more sources to create new services. The term implies easy, fast integration, frequently using open APIs and data sources to produce enriched results that were not necessarily the original reason for producing the raw source data. The main characteristics of the mashup are combination, visualization, and aggregation

g. **Personally-Identifiable Information (PII).** Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.

h. **Social Media.** Media specifically for social interaction that uses highly accessible and scalable publishing techniques using Web-based technologies. Social media use Web-based collaboration technologies to blend technology and social interaction in order to transform and broadcast media monologues into social dialogue, thereby transforming people from content consumers to content producers. These media do not include email.

i. **VA Personnel.** Officers and employees of the Department, consultants and attending physicians, without compensation (WOC) employees, contractors, others employed on a fee basis, medical students and other trainees, volunteer workers without compensation, and trading partners. An attending physician is a physician who has completed residency and practices medicine in a clinic or hospital, in the specialty learned during residency. An attending physician can supervise fellows, residents and medical students. Attending physicians may also have an academic title at an affiliated university such as "professor". This is common if the supervision of trainees is a significant part of the physician's work. Attending physicians have final responsibility, legally and otherwise, for patient care, even when many of the minute-to-minute decisions are being made by subordinates. A trading partner is one of two or more participants in an ongoing business relationship in which any exchange of VA sensitive information takes place.

j. **VA Sensitive Information/Data.** All Department data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive data include the following: individually identifiable medical, benefits, and personnel information; financial, budgetary, identifiable research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information; information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of federal programs.

k. **Viral Marketing.** A marketing technique that uses pre-existing social networks to produce increases in brand awareness or to achieve other marketing objectives through a self-replicating process such as word-of-mouth or via a communication enhanced by the network effects of the Internet.

l. **Web-based collaboration tools/technologies.** The second generation of Web development and design that facilitate communication, secure information sharing, interoperability, and collaboration on the World Wide Web. Web-based collaboration tools are tools that are designed to help people involved in a common task achieve their goals. Web-based collaboration tools include but are not limited to weblogs (blogs), video blogs (vlogs), wikis, hosted services, social networks, video sharing sites, podcasts RSS or Really Simple Syndication (RSS2) feeds, virtual worlds, Web applications, folksonomies, and mashups.

Social Networking Disclaimer

Welcome to the United States Department of Veterans Affairs (VA) **(organization) (website)** page. This page provides a forum for veterans, servicemembers, and their spouses and children to learn how VA **(state activity that the website/page features).**

If you would like to learn more about **(name of VA organization or program)** or if you have specific questions about **(name of organization or program)**, please visit the **(program)** Internet **(or intranet)** site- the official source of information about the **(program)** at **(program website).**

The **(VA organization)** aims to create an open discussion related to the content on this page and encourages helpful and useful comments. We will post and attempt to comment on legitimate questions and concerns regarding the protection, use, storage, or dissemination of personally-identifiable information (PII) or individually identifiable health information (IIHI).

Please note that this is a moderated page, meaning that all comments will be reviewed for appropriate content. Please show respect to those who will read your comments. Comments that do not directly relate to **(topic covered on website/page),** including abusive or vulgar language, spam, hate speech, personal attacks, or similar content will be considered “off topic” and may not be posted on this channel. We reserve the right to determine which comments are acceptable for this page. We will however, post and attempt to comment on legitimate questions and concerns regarding VA's mission and the Department's efforts to provide Veteran benefits, health care, and burial and memorial services.

Be aware that the comments published on all parts of this page—even when the commenter identifies himself or herself as a VA employee—are not to be considered official communications from the Department of Veterans Affairs. The responses, by nature, have to be general. The programs discussed are complicated and most rules will have exceptions and caveats. If you have a specific question about your specific situation, please visit our secure question and answer site.

While VA will not collect or retain these comments in our records, this is a public forum and any information provided in comments may be publicly available on **(name of website)** and the privacy policies of **(name of website)** apply. Please remember that this is a public forum and any information provided in comments will be available to the general public. As such, please do not include personal details such as a veteran file number, social security number, or any other information you do not want to be available to the general public. If you choose to post personal information, you do so at your own risk. VA disclaims any liability for any loss or damage resulting from any comments posted on this page.

This forum may not be used for the submission of any claim, demand, informal or formal complaint, or any other form of legal and/or administrative notice or process, or for the exhaustion of any legal and/or administrative remedy. If you have specific questions regarding a VA program that involves details you do not wish to share publicly please contact the program point of contact listed at https://iris.va.gov.