UNIFORMED SERVICES UNIVERSITY OF THE HEALTH SCIENCES

SUBJECT: Internet Capabilities & Social Media

MAR 29 2013

Instruction 9004

(CIO)

ABSTRACT

This Instruction assigns responsibilities and prescribes procedures for establishing, operating, and maintaining DoD internet services; and the effective and efficient implementation and use of social media associated with the Uniformed Services University of the Health Sciences (USUHS).

A. Reissuance and Purpose.

1. This Instruction provides policies and procedures for the effective use of internet-based capabilities and social media.

B. References. *See Enclosure 1.*

C. Definitions. *See Enclosure 2.*

D. Applicability.

1. This Instruction applies to all faculty, staff, students, contractors including research-funded contract personnel and individuals, and groups who are associated with or are acting on behalf of the University in the management or use of any web and/or social media services or systems. The policies and procedures prescribed in this Instruction apply to the following situations:

a. Any external official presence in a social media application originating from USUHS.

b. Official positions posted on social media applications originating external to USUHS.

c. Unofficial positions taken by individuals who either self-identify with or can be associated with USUHS. For example:

(1) Self-identification is when the individual states as part of the comment or notes in an online profile that he or she is a faculty member at USUHS.

(2) The ability to be associated with USUHS is related to the tenor of the comments rather than the ability of others to Google search the individual's name to establish that association.

2. This policy does **NOT** apply to the following situations:

a. Internal, password-protected social media applications employed by faculty/staff in the educational or administrative functions of the University. For example, blogs and wikis created in a learning management, content management system or in a Google-cloud application do not establish a public presence. Therefore, this policy does not apply because they do not meet the requirements of DoD Instruction 8550.01 *(reference (a))*.

b. A social media presence created by students, faculty, staff or contractors that have not associated themselves with USUHS. These applications are personal rather than an official USUHS presence. They do not meet the statutory requirements for record keeping.

E. Policy.

1. Internet-based Capabilities *(see Enclosure 2 for a definition)* use is permitted and encouraged when it furthers the USUHS mission. However, they shall not be used to collect, disseminate, store or otherwise process non-public USUHS information. Since internet-based capabilities are not subject to Federal or DoD information assurance (IA) standards, controls, or enforcement, they may not consistently provide confidentiality.

a. Use of internet-based capabilities can be either (a) an official external presence that is approved by the USUHS Vice President for External Affairs (VPE); or (b) uses unrelated to public affairs where a USUHS employee is simply acting in his/her official USUHS capacity. Because these uses often take place in a public venue, personnel acting in their official capacity shall maintain liaison with VPE to ensure organizational awareness. In addition, they must:

(1) Ensure that the information posted is relevant and accurate, and provides no information that is not approved for public release including personally identifiable information as outlined in DoD Instruction 5400.11 *(reference (b))*.

(2) Include a disclaimer when personal opinions are expressed (e.g., "This statement is my own and does not constitute an endorsement by or opinion of the Department of Defense or Uniformed Services University of the Health Sciences").

b. Any USUHS-hosted internet services shall be operated and configured to meet the requirements of DoD Instruction 8500.2 *(reference (c))*.

2. Official External Presence (see *Enclosure 2* for definition) shall:

a. Clearly identify that USUHS provides their content and shall comply with DoD Instruction 5400.13 *(reference (d))*.

b. Receive approval from the VPE prior to the presence being established and confirm that the planned use and risks have been assessed and are acceptable. Requests for approval are submitted via an online Social Media Registration Form *(Enclosure 3)*.

c. Be registered on an "external official presence" list which is maintained by VPE. This list should also document the role and scope of the external official presence, i.e. purpose, audience and name of responsible manager.

d. Be registered by VPE on the DoD Social Media registration site *(http://www.defense.gov/RegisteredSites/SubmitLink.aspx)* per DoD Web Policy and DoD DTM 09-026.

e. Use official USUHS seals and logos and provide links to the university's official public website *(www.usuhs.edu)*.

f. Be actively monitored and evaluated for compliance with security requirements (CIO's responsibility) and for fraudulent or objectionable use (VPE's responsibility).

3. Use of Approved Domains.

a. The .mil domain has been established for exclusive use by DoD and should be the primary address for DoD internet services unless the purpose of the internet capability is academic in nature. In those cases USUHS, as an accredited degree granting academic organization, can use the usuhs.edu domain name.

b. USUHS .mil and .edu domain names are not authorized to redirect to non-.mil or non-.edu domain named hosts, (e.g., name .mil will not redirect to name .com or name .org).

c. Only .mil or .edu domain names should be registered by USUHS personnel.

d. As an exception, domain names such as .org, .us, .com, etc. may be registered by USUHS personnel in order to protect a trademark or to prevent domain names from being used in a manner that would be confusing to the public or with conflicting purposes, provided the domain name is held in reserve or used to redirect to the corresponding USUHS .mil and/or .edu domain. A .org, .com, etc. domain name shall not be used as an official USUHS web or email presence; these are restricted to .edu and/or .mil.

e. Exceptions to USUHS .mil and .edu domain name registration to protect a domain name, for research and/or test and development purposes, shall be approved in writing by the USUHS-Designated Accrediting Authority (DAA). Submission of these requests is done through the USUHS Service Desk.

4. Social Media. All USUHS personnel who use social media as an official part of their position or for personal use on a government computer are required to read and comply with this policy. USUHS shall isolate, disconnect, terminate, or otherwise shut down access to a social media presence that is not in compliance with this policy.

a. Individual Access. For the purpose of this policy, individuals are defined as students, faculty, researchers, staff, interns and contractors. Individuals shall have open access to social media sites unless specifically prohibited by DoD policy. They are authorized to create social media accounts for personal use; however, the following provisions apply:

(1) Use non-mission related contact information, such as telephone numbers or postal and e-mail addresses to establish personal accounts.

(2) Comply with standards of conduct on the dissemination and discussion of non-public information.

(3) Do not use personal social media sites to conduct official business.

b. Account Management.

(1) All instances of official external social media presence shall receive approval from the USUHS Office of the Chief Information Officer (OCIO). This approval will be submitted to the USUHS Configuration Control Board (CCB) online using the USUHS Service Desk (select "Request" and then category "Web Social Media"). This approval is required for all administrators for social media applications and signifies that the CIO concurs with the planned use and has assessed risks to be at an acceptable level for using social media technologies.

(2) All instances of social media presence at USUHS shall be registered online with VPE *(Enclosure 3)*. Registration will occur before the social media page is launched.

(3) All instances of social media presence at USUHS shall do the following:

(a) Be clearly identified as part of USUHS through specific statements and/or the use of official USUHS-approved logos.

(b) Provide links to the organization's official public website.

c. Acceptable Use.

(1) There are four broad uses of social media at USUHS:

(a) Official USUHS interests – Official use implies that the use of social media is for the express purpose of communicating USUHS interests or specific programmatic and policy information. For example, the School of Medicine could use Facebook to announce a USUHS-sponsored symposium and then use Twitter during that symposium. There are also many official uses of social media that are not outward facing, such as internal blogs or wikis for collaboration among USUHS project teams or in an individual classroom.

(b) Professional interests – Professional use implies that an individual uses social media for the purpose of furthering specific job responsibilities, research or professional duties through a social media site. For example, almost 30,000 government employees have signed up as members at the external site *GovLoop.com* to engage with other professionals in a community of practice. Another way individuals might engage in social media sites is by

accessing Facebook to view official government pages, such as the DoD or the Chairman, Joint Chiefs of Staff Facebook pages.

(c) Personal interests – Generally, the use of social media for personal interests that are non-official and non-attributable is not covered by this policy. The exception will be when a government computer is used to access a social media site. For example, an individual may want to check their personal Facebook page, send out a personal Tweet, or watch the latest viral YouTube video during a lunch hour or another designated break during work hours. In this case, the relevant sections of this policy apply.

(d) Hybrid – Students, either at the class or seminar level, have the option to create a presence in social media that will potentially address USUHS, professional and personal interests. This presence will help students create enduring connections to other members of their groups and the University. The use of this social media is encouraged. While, as noted above, this type of use is not subject to the direction of this policy, the guidance contained herein is germane.

(2) Internal administrative business or processes will not be conducted on publicly accessible social media sites.

(3) The use of social media in the classroom or in any way that furthers USUHS educational mission is encouraged.

d. Individual Conduct.

(1) Users shall complete Operations Security (OPSEC) annual awareness and training on the risk of information disclosure and apply it to using social media, types of information to share, with whom they can share it, and what not to share.

(2) Across USUHS, federal employees shall comply with all applicable Standards of Conduct under federal, civil, and criminal statutes; federal regulations; and DoD regulations and guidance. Specifically, they shall strive to do the following:

(a) Use every effort to keep interactions factual and accurate. Correct any misrepresentations found about USUHS. Always do so with respect and by using verified information.

(b) Be transparent, open and factually accurate in all interactions.

(c) Provide links to credible sources of information to support interactions, when possible.

(d) Publicly correct any information we have communicated that is later found to be in error.

(e) Be honest about relationships, opinions, and identity. Whenever individuals comment or editorialize in a professional or expert capacity, they must identify themselves and their association with USUHS.

(f) Protect personal privacy and health information. DO NOT share Personally Identifiable Information (PII) or Protected Health Information (PHI) such as name, Social Security number, age, date and place of birth, mother's maiden name, biometric records, military rank or civilian grade, marital status, race, salary, home/office number, driver's license, email addresses, personal phone numbers, medical diagnosis, and other personal information which is linked to a specific individual. (*See reference (b) and (e)*).

(g) Be timely. Ensure that there are routine procedures for checking social media sites and responding to comments and questions.

(h) Avoid arguments. When engaging with someone with an adversarial position, ensure that one's statements are factual, professional, and not disparaging.

(i) Protect trademarks, copyright, and permissions. *(See reference (f)).*

(j) Do not use the USUHS or departmental name to endorse a product, opinion or cause.

(k) Pursuant to the Hatch Act of 1939 (5 U.S.C. 7321-7326, as amended in 1993), do not engage in activities that associate USUHS, its components, or DoD with any partisan political campaign, election, candidate, or cause. Additional information on the Hatch Act of 1939 and its enforcement can be found at the Office of Special Counsel website *(www.osc.gov).*

e. Security. Social media presents a new set of tools for interactive dialog. However, users may make themselves vulnerable by trusting circles of friends and colleagues and disclosing personal facts more readily. Additionally, the use of social media sites lead to a greater web presence, which in turn leads to a greater risk of spam and targeted phishing attacks. This policy will enable USUHS to limit, but not eliminate, the security risks associated with the use of social media.

(1) Social media websites and emerging social media capabilities shall be monitored and evaluated by the Network Operations & Communications (NOC) Information Assurance (IA) team for compliance with security requirements and for fraudulent or objectionable use IAW the references at *Enclosure 1*.

(2) When accessing internet-based capabilities using USUHS resources in an authorized personal or unofficial capacity, individuals shall employ sound operations security (OPSEC) measures per *reference (g)*.

(3) Users shall use good judgment and not click links or open attachments unless they are from a trusted source, given that cyber criminals often pretend to be people they are not in order to deceive individuals into performing actions that launch cyber attacks, download viruses, and install malware and spyware onto computers.

(4) Users shall always use the strongest password combinations allowed, comprised of as many of the combinations of lower and upper-case letters, numbers, and symbols possible. Users shall change passwords frequently and use different passwords for banking and financial sites, and personal web-based email than those for any other site.

f. Content.

(1) Responsibility for establishing, publishing, and updating content will vary as outlined below:

(a) At the University and school level, the purpose will primarily be outreach, and it is a command decision to create the social media presence. In these situations, VPE is responsible for monitoring the content on each USUHS page to ensure that a consistent, mission-focused message is being conveyed and that they are adhering to the Social Media Policy.

(b) When faculty members employ social media in class, they will register the presence with VPE and will be responsible for monitoring the content to ensure adherence to the Social Media Policy.

(2) Under no circumstances will any individual at USUHS permit CLASSIFIED, UNCLASSIFIED CONTROLLED INFORMATION (UCI), or FOR OFFICIAL USE ONLY (FOUO) material to be posted on a social media site. If such material is discovered on a social media site managed by USUHS, it will be immediately taken down and reported to the Security Manager (SEC) and Information Assurance (NOC).

(3) The status of Classified, UCI, or FOUO data does not change as a result of any unauthorized disclosure of identical or similar information on a social media or website (e.g., WikiLeaks) and shall not be posted to or linked from any social media site within the USUHS enterprise *(reference (h))*.

(a) Every individual in the USUHS community who has been granted authorization for access to classified information has affirmed by official classified information nondisclosure agreement (SF-312) to protect this information even if found in unprotected areas.

(b) If Classified, UCI, or FOUO information appears in the public media, DoD personnel must be careful not to make any statement or comment that would confirm the accuracy or verify the classification or status of the information *(reference (i))*.

(4) Whenever possible (e.g., Facebook, LinkedIn, etc.), a formal policy statement will be posted on all USUHS social media *(Enclosure 4)*. The policy statement outlines the purpose of the social media presence, expectations, and content that will be deleted if it includes comments or links associated with any of the following:

(a) Threatening, slanderous, or obscene language.

(b) Personal attacks.

(c) Discriminatory language (including hate speech) based on race, national origin, nationality, age, gender, sexual orientation, religion, or disability.

(d) Sexually explicit material and other material that would violate the law if published on the social media site.

(e) Spam, solicitations, advertisements or undecipherable language.

(f) Comments that suggest or encourage illegal activity.

(g) Personally Identifiable Information (e.g., social security numbers, personal postal and email addresses, personal phone numbers, birth date, birth place, etc. for yourself or others).

(5) Advertisements. Administrators shall coordinate with the OCIO for submitting written requests to social media providers to block the display of any commercial advertisements, solicitations, or links on USUHS official-use accounts if the provider would otherwise normally display commercial advertisements.

(6) Social media is a dialogue. Comments made about USUHS on external social media sites and all comments made by participants on any social media presence across USUHS will require monitoring and evaluation. The content and tone of a comment will determine whether action is necessary. Decision trees addressing options for both external and internal postings are at *Enclosures 5* and *6*, respectively.

g. Disclaimers and Banners.

Place the following message in a prominent location on each authorized page as practicable:

(1) If the social media provider is unwilling or unable to block the display of commercial advertisements, place the following message in a prominent location on each authorized page as practicable:

"The appearance of commercial advertising and hyperlinks inserted by the host of this service does not constitute endorsement by the U.S. Department of Defense/ Uniformed Services University of the Health Sciences (USUHS)/[component]."

(2) Make available or display the standard transparency banner (below) on social media pages, as practicable.

"Welcome to the [Uniformed Services University of the Health Sciences (USUHS) or Component]'s [name of social media] page/presence. If you are looking for the official source of information about the [USUHS or Component], please visit [address of official website or other official information].

The [USUHS or Component] is pleased to participate in this open, un-moderated forum in order to increase government transparency, promote public participation, and encourage collaboration.

Please note that the [USUHS or Component] does not control, moderate or endorse the comments or opinions provided by visitors to this site. The protection, control, and legal aspects of any information that you provided to establish your account or information that you may choose to share here is governed by the terms of service or use between you and the [name of social media provider]. Visit the [USUHS or Component] contact page at [address of official website or other official information] for information on how to send official correspondence."

h. Legal Issues.

(1) DoD DTM 09-026 requires "a process for reviewing information proposed for dissemination … to ensure information is reviewed, cleared, and authorized for release to the public…." USUHS engagement in social media is bifurcated into official and unofficial engagements and VPE serves as the clearing agent for all USUHS official engagements.

(a) Individuals identified as officially speaking for the University or its components must have clearly defined lines that either grant authority to the individual or complete a staffing process for approval and release.

(b) Individuals in an unofficial capacity may choose to engage external participants on social media sites on issues related to USUHS; however, these individuals must make it clear that they are speaking for themselves and not on behalf of the University. If they publish content on any social media or website that has something to do with the work they do or subjects associated with the University, they shall use this disclaimer:

"The postings on this site are my own and do not necessarily represent the positions or opinions of the Uniformed Services University of the Health Sciences (USUHS) or the Department of Defense."

(1) By posting content to any social media site, individuals agree that they own or otherwise control all of the rights to that content, that use of the content is protected fair use, that they will not knowingly provide misleading or false information, and that they indemnify and hold the University harmless for any claims resulting from the content. To the maximum extent possible, posting online material that includes direct or paraphrased quotes, thoughts, ideas, photos, or videos, shall include citations. Provide a link to the original material, if available.

(2) The Hatch Act of 1939 prohibits federal employees from engaging in partisan political activity; therefore, any postings that lobby or campaign for a political issue, party, or candidate will be removed and the employee posting said material may be subject to appropriate administrative or punitive action. Penalty for violation of the Hatch Act is removal from Federal Service, but it may be mitigated to a minimum 30 day suspension by the Merit Systems Protection Board (MSPB) (5 USC 7326).

i. Privacy.

(1) If there is a survey or any other vehicle posted on a USUHS social media site that requests individuals "to furnish personal information and the information is to be included in a Privacy Act system of records (i.e., a system in which information about the individual is retrieved by name or other personal identifier)," a Privacy Act statement "must be posted or provided through a well-marked hyperlink on the page where the information is being requested" *(reference (j))*.

(2) If an individual is requested to give personal information and that information is not maintained in a Privacy Act system of records, the solicitation of such information requires a *privacy advisory*. The privacy advisory informs the individual as to why the information is being solicited and how it will be used. The privacy advisory will be posted on the page where the information is being requested or provided through a well-marked hyperlink *(reference (j))*.

(3) Any question regarding PII loss or suspected loss of PII shall be reported immediately to the Privacy Act Officer in the Office of Accreditation and Organizational Assessment (OAC).

(4) USUHS shall have the right to remove any content for any reason, including but not limited to, content that it deems threatening, obscene, a violation of intellectual property rights or privacy laws, or otherwise injurious or illegal. Content that is simply critical of USUHS or its components shall NOT be removed. *Enclosure 5 and 6* contain response decision trees.

5. Process & Procedures.

a. Creating social media presence.

(1) Development Guide. Social media is constantly evolving, so no specific guidance for development is addressed in this document. However, the DoD Social Media Hub at *(http://www.defense.gov/socialmedia/)* is an excellent resource that provides up-to-date practical steps based on best practices and official policies on how to develop and use social media effectively.

(2) Seals and logos. Only official USU seals and logos shall be used. All seals/logos must be approved by VPE.

(3) Role and scope. All social media sites within the USUHS enterprise shall clearly indicate their role and scope.

(4) Links. When possible, all official social media presence shall do the following:

(a) Provide links to the USUHS official public website and, when appropriate, the subordinate school/department's official public website. Student classes and seminars are encouraged to provide similar links.

(b) List USUHS and School social media pages as "favorites." Links are permissible to any non-DoD site that offers information or services related to the function or mission of an USUHS enterprise social media presence; however, non-DoD links require the following disclaimer:

"The appearance of hyperlinks does not constitute endorsement by the Department of Defense, Uniformed Services University of the Health Sciences (USUHS), or its components of non-United States Government sites or the information, products or services contained therein. While the USUHS and its components may or may not use these sites as additional distribution channels for Department of Defense information, it does not exercise editorial control over all of the information that you may find at these locations. Such links are provided consistent with the stated purpose of this [website/social media application]."

b. Oversight.

(1) There are two primary reasons for oversight: activity and compliance.

(a) Activity. The hallmark of social media is the dialogue generated. If there is not oversight (e. g., somebody checking to see if there is a question or comment needing response, periodic postings, etc.), the dialogue ends and the site dies.

(b) The administrator for each social media presence shall ensure that it is checked daily and they shall document activity as outlined in paragraph 5.c. below.

(2) Compliance. It is equally important to ensure that all social media sites within the USUHS enterprise are in compliance with this policy. Although VPE has ultimate oversight, the school or department level social media managers have primary responsibility, and administrators shall routinely monitor all social media sites under their purview for the following:

(1) Overall compliance with the content, conduct, legal, and security policies of USUHS.

(2) Periodically verify all external links to ensure the link is still available and that the link continues to provide quality (i.e., objectivity, utility, integrity, etc.) information. Solely relying on automatic link validation tools is not sufficient, and manual review of the content at external links is required. If the content of a linked external site becomes outdated, questionable, or objectionable, remove it.

(3) The NOC Information Assurance (IA) team shall periodically monitor and evaluate social media sites for compliance with security requirements and for fraudulent or objectionable use.

c. Documentation and records. USUHS is subject to records requirements of the Freedom of Information Act (FOIA). There are nine exemptions to the law that range from withholding data "specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy" to "clearly unwarranted invasion of personal privacy." Since Classified, UCI, or FOUO documents shall not be placed in social media, and there is no expectation of privacy in social media, USUHS social media applications are subject to the law and records must be maintained.

(1) Edits/Removals. As outlined in *Enclosure 5 and 6,* there are occasions when a posting must be edited or completely removed. In those instances, the following must be reported:

(a) A record of the original posting and, if applicable, its edited version.

(b) Date and time the posting occurred.

(c) Date and time the posting was removed or edited.

(d) Reasons for the action taken.

(2) Reports shall be submitted to VPE and/or NOC Information Assurance (if security issues apply) and can be submitted via an online "Social Media Edit Record Form." VPE shall brief the USUHS Chief of Staff on all removal/editing actions.

(3) Annual archiving. The FOIA requirements for public access to information from within the executive branch create a need for documentation and archiving of social media activity *(reference (k))*. Social media administrators are responsible to do the following:

(a) Electronically capture all activity on their social media sites. The periodicity of this capture may vary with the volume of traffic on a given site, but shall be no less than quarterly.

(b) Submit a compilation of captured traffic to VPE quarterly.

F. Effective Date. This Instruction is effective immediately.

Charles L. Rice, MD
President

Enclosures:
1. References
2. Definitions
3. USUHS Social Media Registration Form
4. Example Social Media Comments Policy
5. Response Assessment Decision Tree (External)
6. Response Assessment Decision Tree (Internal)
7. Google+ Usage Guide
8. Social Media Edit Form

REFERENCES

(a) DoD Instruction 8550.01, "DoD Internet Services and Internet-based Capabilities," dated September 11, 2012.

(b) DoD Instruction 5400.11, "DoD Privacy Program," dated September 1, 2011.

(c) DoD Instruction 8500.2, "Information Assurance Implementation," dated February 6, 2003.

(d) DoD Instruction 5400.13, "Public Affairs (PA) Operations," dated October 15, 2008.

(e) DoD Instruction 8580.02-R, "DoD Health Information Security Regulation," July 12, 2007.

(f) USUHS Instruction 5536, "Copyrights and Royalties," dated September 24, 2009.

(g) DoD Manual 5202.02-M, "DoD Operations Security (OPSEC) Program Manual," dated November 3, 2008.

(h) Executive Order 13526, Section 1.1 (4) (c), "Executive Order-Classified National Security Information," dated December 29, 2009.

(i) DoD Instruction 5200.1-R: C10.1.2.3., "Information Security Program," dated January 14, 1997.

(j) Directive-Type Memorandum 09-026, "Responsible and Effective Use of Internet-based Capabilities," dated February 25, 2010.

(k) DoD Instruction 5015.2, "DoD Records Management Program," dated March 6, 2000.

(l) DoD Instruction 8500.01E, "Information Assurance (IA)," dated April 23, 2007.

(m) ASD Memorandum "Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites," dated December 28, 2001.

(n) DoD Instruction 8410.01, "Internet Domain Name Use and Approval," dated April 14, 2008.

(o) Hatch Act of 1939 (5 U.S.C. 7321-7326, as amended in 1993).

(p) DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," dated November 28, 2007.

(q) USUHS Instruction 5203, "USUHS Civilian Personnel Security and Suitability Investigative Program," dated November 5, 2006.

DEFINITIONS

1. Internet-based Capabilities. All publicly accessible information capabilities and applications available across the internet in locations not owned, operated, or controlled by the Department of Defense or the Federal Government. Internet-based capabilities include collaborative tools such as Social Networking Service (SNS), social media, user-generated content, social software, e-mail, instant messaging, and discussion forums (e.g., YouTube, Facebook, MySpace, Twitter, commercial email such as Yahoo, etc.).

2. Official External Presence. Official public affairs activities conducted on non-DoD sites on the Internet (e.g., USUHS VPE on Facebook and Twitter).

3. USUHS Public Website. USUHS public websites are information resources funded in whole or in part by the Federal government and/or operated by USUHS, contractor, or other organizations on behalf of USUHS.

USU SOCIAL MEDIA REGISTRATION FORM

USUHS Social Media Registration Form

To be completed and submitted to the Vice President for External Affairs (VPE) before official launch of any USUHS branded social media presence.
Your username (@usuhs.edu) will be recorded when you submit this form. Not **timothy.rapp**? Sign out
* Required

GENERAL INFORMATION

1. Department? *
Three-letter departmental code, e.g. ASD, APG, MEM, etc.

2. Type of Social Media *
- ☐ Facebook
- ☐ Twitter
- ☐ Blog
- ☐ LinkedIn
- ☐ Other

If "other", please describe and/or provide URL

3. Social Media Title *
Please enter the title of the USUHS Social Media presence, e.g. "Official School of Medicine Facebook Page"

4. Social Media URL *
The web address of the social media presence.

5. Desired Launch Date *
In MM/DD/YYYY format

The complete form can be found at: *http://goo.gl/qKPIm.*

USUHS Instruction 9004, 3/2013

EXAMPLE SOCIAL MEDIA COMMENTS POLICY

Welcome to the official [insert name of social media presence].

We hope you will find our page to be a useful source of news updates and information about USUHS activities, events, publications, and programs. We also hope it will become a place for you to connect, make friends, and be a part of our online community. We recognize that it's your community. But we also want you to be cognizant that it is an OFFICIAL page for the Uniformed Service University of the Health Sciences (USUHS) or one of its components, which are all part of the U.S. Department of Defense.

This is an open academic forum. This is not the place for personal attacks, spam or rants. Per our comments policy, we will delete comments if they include any of the following:

- Threatening, slanderous, or obscene language
- Personal attacks
- Discriminatory language (including hate speech) based on race, national origin, age, gender, sexual orientation, religion or disability
- Sexually explicit material and other material that would violate the law if published here
- Spam, solicitations, advertisements, or undecipherable language
- Comments that suggest or encourage illegal activity
- Personally Identifiable Information (e.g., name, Social Security number, age, date and place of birth, mother's maiden name, biometric records, military rank or civilian grade, marital status, race, salary, home/office phone numbers, and other personal information which is linked to a specific individual.)

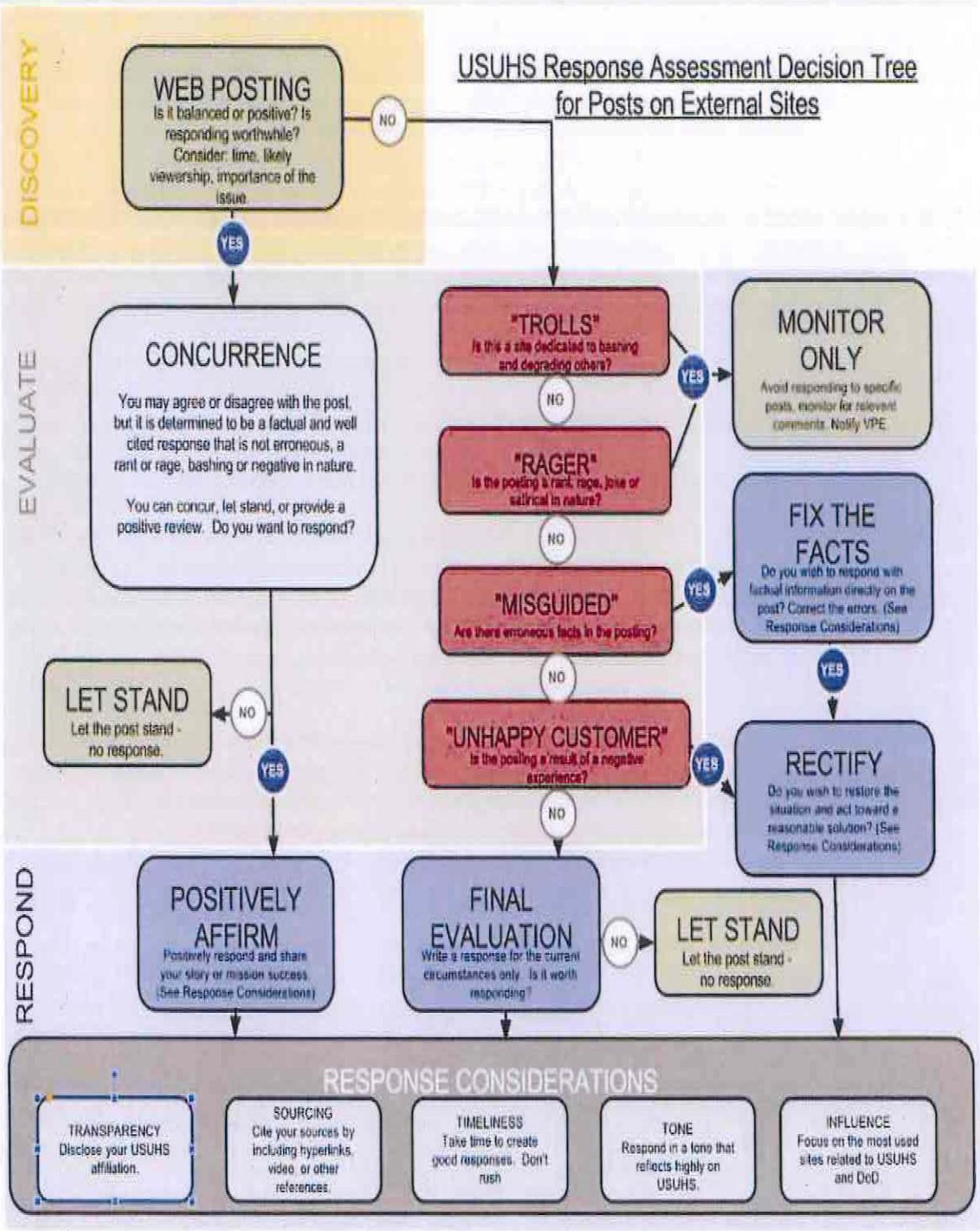
Please participate at your own risk, taking personal responsibility for your comments. The appearance of external, non-USUHS links on this site does not constitute official endorsement on behalf of USUHS, the Assistant Secretary of Defense for Health Affairs (ASD (HA)), or the U.S. Department of Defense. USUHS does not guarantee or warranty that the information posted by individuals on this site is correct, and disclaims any liability for any loss or damage resulting from reliance on any such information.

Media requests and questions should not be submitted here. We ask that you submit your questions through our normal USUHS Public Affairs channel at *(http://www.usuhs.mil/vpe/mediaaffairs.html)*. Any posts with media requests/questions will not be responded to and will be removed.

While social media is a 24/7 medium, our moderation capabilities are not. We may not see every comment right away, and we trust in the dignity of our community to respond to personal attacks and negative speech politely or to ignore them.

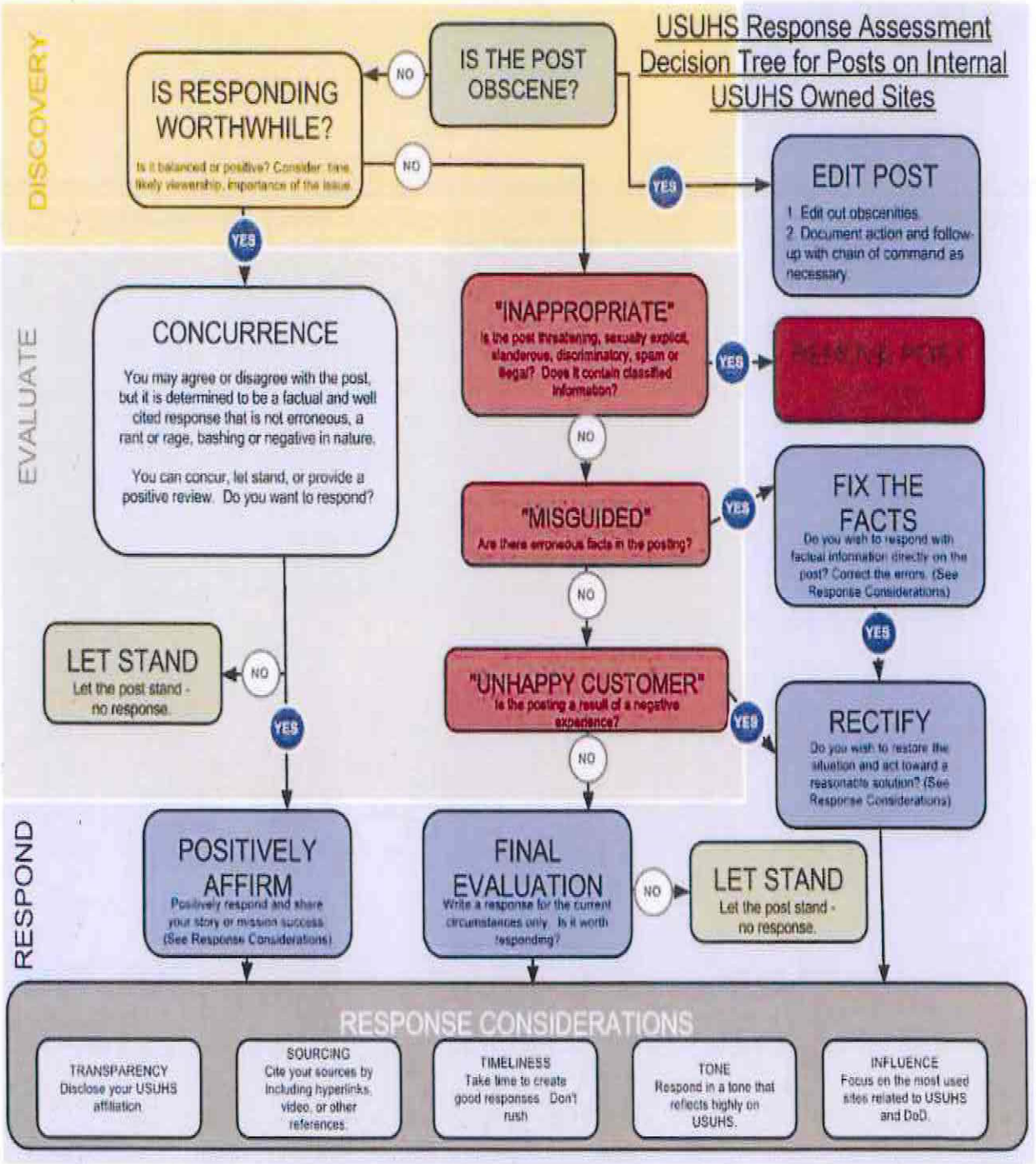
Keep commenting and thanks for joining the conversation.

RESPONSE ASSESSMENT DECISION TREE (EXTERNAL)



The full diagram is available at: *http://goo.gl/EjI6t*.

RESPONSE ASSESSMENT DECISION TREE (INTERNAL)



The full diagram is available at: *http://goo.gl/UUmU5*.

GOOGLE+ USAGE GUIDE

1. Google+ is a constantly evolving social media tool with the purpose of sharing information with others. These consistent changes and rapid updates quickly make any specific step-by-step policies and procedures obsolete. As a result only general Google+ guidance will be offered in this policy document.

2. General Usage Guidance.

a. As with any social interaction, good judgment and effective communication are required.

b. To use Google+, users must create a Google+ profile, which is publicly visible to anyone on the web. However, each user can choose which information in their profile to share publicly or with just specific circles, and which information to keep private.

c. The default setting for USUHS Google Apps for government (Gov) accounts should only be privately shared information. Decisions to post publicly should be made for each individual post preventing inadvertent public sharing. For example, circles are private by default. Be deliberate in who you add to your circles and what information you add to your profile. If it's not public information, do not add it.

d. Limit who can contact you from your Google+ profile. From your Google+ screen click on "Profile", "Edit profile" and then "Change contact settings." From here you can limit who can contact you from your profile from no one to USUHS only to public.

3. A more detailed *Google+ best practices guide* is available and maintained on the USUHS One-Stop Intranet Site *(onestop.usuhs.edu)*.

SOCIAL MEDIA EDIT FORM

Social Media Edit Record

Please submit this form any time you as the Social Media manager or administrator must edit or remove a posting because it does not comply with current DoD and/or USUHS policy (see USUHS Instruction 9004). Submission of this "Social Media Edit Record" is to meet Freedom of Information Act (FOIA) compliance requirements.
Your username (**timothy.rapp@usuhs.edu**) will be recorded when you submit this form. Not **timothy.rapp**? Sign out
* Required

1. Please insert a copy of the original post *

2. Please insert a copy of the edited version
If applicable

3. Date the posting occurred? *

4. Date and time the posting was removed or edited? *

5. Reason the action was taken? *

The complete form can be found at: *http://goo.gl/suS16.*