SAMHSA Policy for Official Use of Social Media

Office of Management, Technology and Operations

4/18/2012

Table of Contents

1 Purpose

The purpose of this Substance Abuse Mental Health Services Administration (SAMHSA) document is to establish policy for the use of Third-Party Websites and Applications (TPWAs), social media and related technologies as part of any general support or application system and to incorporate by reference related Federal-government-wide guidelines and SAMHSA policies. In effect this policy changes the default from avoiding use of TPWAs except when a specific business case is approved to embracing TPWAs unless a specified risk must be avoided.

2 Disclaimer

It is SAMHSA policy that Agency personnel abide by or exceed the requirements outlined in this document. In cases where personnel, contractors, and other authorized users cannot comply with the SAMHSA *Policy of Official Use of Social Media* for technical or financial reasons, or because it precludes the personnel, contractors, or other authorized users from supporting their mission or business function, justifications for the noncompliance will be documented using a policy waiver form and submitted to the Chief Information Officer (CIO) for approval.

3 Background

In August 1, 2010 SAMHSA published the first social media policy that established limited restricted access to approved TPWA's and social media sites with approved business cases. To ensure security and privacy, official SAMHSA social media use was separated from the main SAMHSA network using SAMHSA owned laptops for access and use.

On March 7, 2012, the Health and Human Services (HHS) Department issued a new policy for social media technologies which allows greater access to social media. The new policy establishes the allowance of and access to social media and other third party hosted websites and applications (TPWA) that are used to fulfill SAMHSA's mission. The new HHS policy directs SAMHSA to default to maximum access to social media sites, third party websites and applications (including YouTube, Twitter, Facebook and other mainstream social media sites).

The decision to allow the use of TPWA's was made by the HHS Chief Information Officer after the General Services Administration (GSA) announced they have established terms of service agreements (TOS) that set Federal standards by which the TPWA providers must adhere. This will ensure the Government's trust in that site, including IT security.

4 Scope

This policy applies to all SAMHSA staff, including all SAMHSA personnel, contractors, and other authorized network users. This policy does not supersede the Health and Human Services Office of the Secretary Office of the Chief Information Officer (HHS OS OCIO) policy for social media technologies or higher level agency or federal directives in effect as of the effective date of this policy. This policy does replace the SAMHSA Official Use of Social Media Policy published in May 12, 2010.

5 Policy

Access to TPWAs shall default to the maximum access assessed acceptable to the SAMHSA Chief Information Officer (CIO).

Terms of Service (TOS) agreements for use of any TPWAS shall default to the TOS agreement executed between the HHS Department and the TPWA provider. These default TOS agreements shall be based on the models negotiated for the Federal government by the General Services Administration.

SAMHSA is permitted to make a risk based decision on the value and need to deviate from the Departmental access standard for a given TPWA or the default TOS agreement for a given TPWA. SAMHSA may request a waiver to either further open or further restrict access or to alter a TOS agreement. For waiver requests to further restrict access from an established HHS Departmental standard, the SAMHSA CIO is authorized to temporarily implement the requested further access restrictions pending adjudication of the waiver.

6 Responsibilities

6.1 SAMHSA Chief Information Officer (CIO)

The SAMHSA CIO is responsible for providing the level of access defined in each TPWA access standard established by the HHS Chief Information Officer, unless a specific waiver is granted. SAMHSA's CIO is required to comply with the access standard for a given TPWA within 30 days of the notification from the HHS CIO that an access standard has been established.

SAMHSA's CIO is responsible for defining the risk justifying any waivers they submit requesting deviation from the access standards or TOS agreements. The SAMHSA CIO is also responsible for defining how the requested deviation from the access standard or TOS agreement will be implemented if the waiver request is granted.

The SAMHSA CIO is responsible for reviewing and adjudicating waiver requests.

6.2 Information Security Assurance Team (IT Security Team)

SAMHSA Information Security Assurance Team is responsible for assisting in establishing access standards for TPWAs. The IT Security Team is responsible for assisting the CIO with the review and adjudications of a waiver request.

The SAMHSA IT Security Team is responsible for maintaining the list of granted waivers for the access standards and TOS agreements, along with the risk assessments and implementation descriptions submitted by SAMHSA.

6.3 Office of Communications (OC)

The Office of Communications (OC) is responsible for posting and managing the content on SAMHSA's official social media sites and vetting all potential information posted on these sites. OC determines what personnel should be granted access and have the ability to upload information and maintain official social media sites on SAMHSA's behalf.

7 Social Media Use

7.1 Access to Social Media

Access to social media and other third party hosted websites and applications are being enabled as a tool to assist staff in helping to fulfill SAMHSA's mission. The same rules that govern use of the Federally-issued computer in accessing internet sites also apply to social media sites. The SAMHSA Internet Rules of Behavior permits the use of the internet, and now social media sites, for business purposes and restricts personal use to lunch and non work hours. Staff must exercise common sense, good judgment, and propriety with the use of government-provided resources. Employees who misuse government resources in any way may have Internet/social media privileges withdrawn and may be subject to disciplinary action. The SAMHSA Rules of Behavior are posted at http://intranet.samhsa.gov/IT/security.aspx

In addition, there are specific ethics rules related to posting on social media which are covered in the SAMHSA annual mandatory HHS ethics training. Of importance -- when you communicate using social media in an official capacity, you represent SAMHSA and may state only authorized messages. Also, your posts on personal accounts should not use any language that implies that the statements represent official SAMHSA views or opinions.

7.2 Social Postings

The Office of Communications (OC) manages SAMHSA's official social media properties (http://www.samhsa.gov/socialmedia/). These accounts are used to support work across the breadth of SAMHSA's mission and OC encourages staff to consider submitting information for posting.

7.3 Appropriate Use

Users who are maintaining SAMHSA social media sites shall understand the distinction between acceptable personal use and the use of social media as part of business/work. Therefore:

- OC shall approve any data that is to be posted on social media sites on SAMHSA's behalf.
- No personally identifiable information (PII) or sensitive data shall be posted on SAMHSA's social media sites.

- Accounts maintained on SAMHSA's behalf must remain professional, appropriate, accurate, and consistent with SAMHSA's mission.
- SAMHSA social media sites and content must clearly identify ownership or sponsorship through the use of SAMHSA branding, which must be part of the approval process.
- Through the terms of services that have been established by the GSA, SAMHSA shall carefully manage the type of information released.
- Information shall be appropriately vetted through OC to prevent disclosure of private and sensitive information.
- All SAMHSA employees are prohibited from creating unofficial SAMHSA accounts to falsely represent SAMHSA, and from falsely posting information that claims to be approved and posted by the agency.
- Employees establishing personal social media accounts must obtain approval from OC before incorporating SAMHSA identifiers, such as official badges or logos, into their profile or user name (i.e., scott@samhsa).
- The SAMHSA public website includes a social media information page listing official SAMHSA social media accounts. This page can be found at http://www.samhsa.gov/socialmedia/. Any sites not listed on this page are not officially sponsored by SAMHSA.

Additionally, SAMHSA employees must know and follow SAMHSA and Executive Branch conduct guidelines, such as *Standards of Ethical Conduct for Employees of the Executive Branch*. These standards prohibit activities such as the use of vulgar or abusive language or offensive terms targeting individuals or groups, and the endorsement of any commercial products or political parties on social media sites.[1] As with all other official communication, social media needs to be conducted in conjunction and coordination with other elements of an office's communication plan. As such, it needs to consider the target audience and what social media tools and practices will be most effective in reaching them. Offices that are considering using social media should contact OC at newmedia@samhsa.hhs.gov to discuss how to most effectively reach their target audience.

8 Wavier Process

8.1 Request to Restrict TPWA Access

There will be a waiver process in place to restrict access if SAMHSA deems it necessary to block a TPWA. A waiver request to block TPWA access can be filed by sending an e-mail with justification to Bill Reed, SAMHSA Chief Information Officer, DTM/OMTO (Bill.Reed@samhsa.hhs.gov)

[1] **Social Media Policy - GSA Order CIO P 2106.1**

8.2 Request to Add TPWA Access

If you find you cannot access a TPWA, and there is a valid SAMHSA business reason to support access to the site, you can file this request with the SAMHSA Chief Information Officer. If approved, the Office of Management, Technology and Operations (OMTO) will work to develop a term of service agreement to allow access.

9 Applicable Laws and Regulations

9.1 Safeguarding SAMHSA Information Resources

Information Technology Security risks associated with use of social media technologies are manageable within a defense-in-depth strategy described by the Federal CIO Council in the Guidelines for Secure Use of Social Media by Federal Departments and Agencies Version 1.0: (http://www.cio.gov/Documents/Guidelines_for_Secure_Use_Social_Media_v01-0.pdf).

Information Technology Security policies and standards to implement a defense-in-depth strategy are numerous and include the SAMHSA-OCIO Policy for Information Systems Security and Privacy, the SAMHSA Standard for Managing Outbound Web Traffic, the SAMHSA Rules of Behavior and the SAMHSA-OCIO Policy for Personal Use of Information Technology Resources.

9.2 Terms of Service Agreements

The General Services Administration, in collaboration with other Federal Agencies, drafted model Terms of Service Agreements for a number of TPWAs. The list of model agreements is available at the URL below.

http://www.usa.gov/webcontent/resources/tools/TOSagreements.shtml

9.3 Privacy

Privacy requirements for TPWAs are unique. SAMHSA policy and requirements closely follow the Office of Management and Budget (OMB) Memorandum 10-23, Guidance for Agency Use of Third-Party Websites and Applications available at: http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf.

10 Contact

Direct all questions, comments or suggestions concerning this policy to the SAMHSA CIO, at Bill.Reed@samhsa.hhs.gov .

11 Effective Date

The effective date of this Policy is the date the Policy is approved.

12 Approved:

/s/ _____

Bill Reed
SAMHSA Chief Information Officer

DATE