1010 Social Media and Agency Communications

I. Purpose

This policy outlines state and federal regulations regarding social media accounts of current and prospective state employees (*See* Ark. Code Ann. § 11-2-124) and establishes guidelines regarding DHS agency communications as well as employee communications, both of which must protect confidential information at all times, including when using social media. For purposes of this policy, "social media account" **does not** include an account:

(A) Opened by an employee at the request of DHS;

(B) Provided to an employee by DHS such as DHS email or other software programs owned or operated by DHS;

(C) Set up by an employee on behalf of DHS; or,

(D) Set up by an employee to impersonate DHS through the use of the DHS name, logo, or trademarks without agency authorization (*See* Ark. Code Ann. §11-2-124 (B)(i-iv).

II. Social Media Policy

(A) DHS employees must never share, post, or expose confidential information about DHS clients, patients, partners, or other employees on any publicly accessible website or social media account.

(1) Social media account refers to a personal account with an electronic medium or service (such as Facebook, Twitter, LinkedIn, Instagram, YouTube, Snapchat, etc.) where users may create, share, or view user-generated content, including without limitation: videos, photographs, blogs, podcasts, messages, emails, and website profiles or locations.

(2) Confidential information includes, without limitation, client medical, health, or personal information, photographs (even modified), recordings (audio and video), or case information.

(3) Such incidents must be reported to the DHS Privacy Office on DHS Share or by clicking here (http://kadril.dhhs.arkgov.net/itsec5/incidentreportform.aspx) and are subject to disciplinary action, including immediate dismissal, as outlined in DHS Policy 4002, "Privacy and Security Sanctions."

(B) DHS will not require, request, suggest, or cause a current or prospective employee to:

(1) Disclose his or her username and/or password to a personal social media account except as outlined in this policy;

(2) Change the privacy settings associated with his or her personal social media account or to list or share the contacts associated with his or her personal social media account; or,

(3) Add another employee, supervisor, or administrator to the list or contacts associated with his or her personal social media account.

(C) DHS will not take action against or threaten to discharge, discipline, or otherwise penalize an employee for exercising his or her rights to post personal opinions on social media, with the following exceptions:

(1) Agency confidential information must not be posted, published, or shared; and,

(2) The employee should refrain from posting on social media sites while on duty. Employees can be held accountable for failing to perform work or assignments while on duty. Evidence of posting on social media while on duty may be used against employees in such cases.

(D) DHS employees may face disciplinary action for posting comments to social media while off duty if the statements contain information gained through their official capacity and threaten or harass others. Harassment refers to any unwelcome, repetitive behavior intended to threaten, disturb, or upset another person. Harassment of others is prohibited at DHS and may be addressed through disciplinary, security, legal, or other action. (Refer to DHS Policy 1009 "Equal Opportunity Policy.")

(E) This policy does not prohibit DHS or any of its employees from viewing information about a current or prospective employee that is publicly available on the internet.

(F) Employees must not use a DHS email address for obtaining and maintaining personal social networking accounts. Employees should use personal email addresses for personal social media.

(G) DHS investigators may request an employee's username and password for the purpose of accessing a social media account if the employee's social media account activity is reasonably believed to be relevant to a formal investigation by DHS Internal Affairs/Fraud or the DHS Privacy or Security Offices for a violation of federal, state, or local laws or regulations or this agency's policies. The employee's username and password must only be used for the formal investigation or a related proceeding.

(H) If DHS inadvertently receives an employee's username, password, or other login information to an employee's social media account by using an electronic device provided to the employee by DHS or a program that monitors DHS' network, DHS is not liable for having the information but may not use the information to gain access to an employee's social media account.

(I) Employees must request, through their office or division chain of command, access to social media sites at work for specific investigative purposes.

III. Agency Communications

Staying Informed

Employees are responsible for staying informed on agency issues and policies through the internal communications available to them (such as DHS Share) and for seeking additional information from their supervisors when needed. Employees can access DHS Policies by clicking here (https://dhsshare.arkansas.gov/DHS%20Policies/Forms/By%20Policy.aspx).

Office of Communications and Community (OCCE) Engagement

(A) Employees shall direct all media questions to the OCCE.

(B) OCCE shall manage all internal and external communications and publications on behalf of DHS. This includes, without limitation:

(1) DHS websites and social media accounts;

(2) Public websites and other social media outlets;

(3) DHS employee newsletters; and,

(4) All communications with news media, specifically, news releases and interviews on behalf of the agency.

(C) OCCE may post information, photographs, or videos about agency clients on DHS websites, social media, or publications if OCCE has obtained permission and signed consent of the client. (The agency consent form must have prior approval of the DHS Privacy Officer.)

(D) Divisions and Offices must consult with OCCE for input when preparing for new communications or community outreach projects.