



A close up of a logo

Description automatically generatedA screenshot of a cell phone

Description automatically generated

**Social Media Guidelines**

**Introduction to Social Networking Sites:**

»» Social Networking Sites are among the most popular components of Web 2.0, which is the second generation of the World Wide Web that allows individuals to interact and share information online. At various SNS, individuals can create personal profile pages, that may include pictures, video, and postings on personal interests.

»» These sites allow each user to maintain a list of friends who may also post messages on his/her profile page.

»» A user can choose who has access to the information posted on his/her profile page (e.g. users on the same network or group, confirmed friends, the general public).

**Global Social Media Trends:**

»» According to a February 2012 press release from *ComScore*, Facebook more than tripled its U.S. visitors from 54.5 million in December 2008 to 163.5 million in December 2012. (Worldwide, Facebook draws 845 million monthly active users, and is available in more than 70 languages).

»» According to a June 2010 World Internet Usage Statistics News and Populations Stats, approximately 1.966 billion people use the internet.

»» According to the Department of Homeland Security, cyber attacks against the government and private networks increased from 4,095 in 2005 to 72,065 in 2008.

»» Nearly sixty-three percent of American adults maintain a profile on SNS. Nearly eighty percent have use privacy settings to restrict access by strangers, according to a February 2012 survey by the Pew Research Center.

»» The Federal Trade Commission estimates that as many as 200,000 million Americans had their identities stolen in 2011.

»» According to *Alexa.com,* one of the largest web crawls, Facebook was the second most trafficked site in the world as of March 2011, as well as the top photo-sharing site with 10 billion photos uploaded.

»» A recent study by the National Cyber Security Alliance reported that although 57 percent of individuals on SNS admit to worrying about becoming a victim of cyber crime they still provide information that may put them at risk.

»» According to *Technorati,* a leading blog search engine and directory, there are 112.8million blogs and 250 million pieces of tagged social media online. More than 175,000 new blogs are created each day.

»» Seventy-eight percent of American adults (age 18 and older) use the Internet.

»» Sixty-three percent of all American are part of a wireless, mobile population that participates in digital activities away from home.

»» Facebook and other popular SNS have developed applications that can identity a user's information. Home addresses, for example, can be found and mapped within a matter of seconds. Location services have become extremely popular as more people take advantage of smart phones with GPS and other mapping capabilities. The Facebook application can either be downloaded or viewed via the mobile Facebook page, and its settings can be changed manually to allow 'friends of friends" or the general! public to view a user's personal information.

**Guidelines:**

*The guidelines below have been provided to increase awareness of the potential threats and risks that employees may experience when accessing SNS on personal, non-government systems. SNS, web pages, email accounts, and wireless access points are all vulnerable to identity theft and information aggregation. Adversaries Include hackers, foreign intelligence agents, terrorists, and criminals who may target your family, friends, neighbors, and/or coworkers.*

»» SNS are a counterintelligence (CI) and operations security (OPSEC) concern because critical, sensitive, and/or personal information may inadvertently be disclosed. FBI personnel should be careful when providing any information online about themselves, their organization, or their lob. They should refrain from disclosing on any section of their user profiles that they work for the FBI or the Department of Justice. FBI personnel must also consider each word that they post, as these posts will remain indefinitely in cyberspace.

»» FBI personnel shall not promote their personal or professional importance in profile(s) or posting, as this may make them a potential target for adversaries to exploit.

»» FBI personnel should not provide details regarding their work associates, official position, or duties.

»» FBI personnel shall not advertise weaknesses, vulnerabilities, or loopholes within FBI systems or capabilities.

»» FBI personnel shall limit the amount of personal information that they post on SNS. Do not post information that would make you vulnerable, such as your home address or information on your schedule/routine (e.g. on Twitter or LinkedIn). If your friends or connections post information about you, make sure that the combined information is not more than you would be comfortable with strangers knowing. Also be considerate when pasting information on your connections, including photographs (e.g. on Facebook, MySpace, or dating websites).

»» FBI personnel are prohibited from using FBI Information Systems (IS) to access publicly accessible SNS for non-FBI business purposes.

»» FBI personnel who access SNS for personal use from non-FBI IS (e.g., home or publicly available IS) shall not disclose information pertaining to FBI operations or any other information gained by virtue of FBI employment, either during or after their tenure of service with the FBI. This includes photographs or videos involving official FBI related matters and/or FBI facilities.

»» FBI personnel shall not establish any publicly accessible SNS that represents itself as an official FBI site or as affiliated with the FBI.

»» FBI personnel shall not use or associate official FBI email accounts with personal social networking accounts.

»» FBI personnel shall comply with the FBI Seal, Name, Initials and Special Agent Gold Badge Policy, Corporate Policy Directive 0266D, regarding any use of the FBI Seal, Name, Initials or Special Agent Gold Badge, to include use on publicly available SNS.