Guidelines for Employee Use of Social Media

This document is designed to offer employees of Huntington Ingalls Industries (HII) practical and helpful guidance for responsible, constructive communications via social media channels.

HII is active in social media, including on Facebook, Twitter, Instagram, LinkedIn and YouTube (go to http://www.huntingtingalls.com/social for a complete list) and encourages employees to participate themselves during non-work hours on non-work equipment.

Employees should not access social media sites during their working hours. Only HII employees whose jobs require using social media are given access to these sites on HII networks. Outside of their working hours, employees may use social media through non-HII computer systems and networks.

Social networks are a great way to connect with others personally and professionally, but you should be wary about the security of your personal information.

To protect HII’s security, integrity and brand:

- Only HII Corporate Communications may create and maintain company-branded social media profiles. Please refer to Procedure “Company Sponsored Social Media Channels” (A604) on Corporate Command Media.
- Only those officially designated may use social media to speak on behalf of our company in an official capacity, though employees may use social media to speak for themselves individually.
- Employees are responsible for making sure their online activities do not interfere with their ability to fulfill their job requirements or their commitments to their managers, co-workers or customers. As such, only HII employees whose jobs require using social media are given access to these sites on HII networks.
- Do not use company e-mail addresses to create social media profiles, and do not associate company e-mail addresses with social media profiles.
- Don’t use the same passwords for your HII login credentials and your social media profiles.
- Do not send or post on social media any of HII company confidential information, including but not limited to proprietary information, trade secrets, and business plans or processes; government classified information; and export-controlled information.
- Do not post any command media, internal communications, reports or presentations to the extent such postings contain, reference, reflect or are based on company confidential information.
- Do not post photographs, video or audio of other HII employees, suppliers, customers or agents without first obtaining their approval.
- Do not use HII logos, trademarks or proprietary graphics without the company’s express prior written permission.
• None of these rules are intended to restrict employees from using social media to participate in activities otherwise protected by law, including the right to discuss employees’ terms and conditions of employment.
• If an employee is in doubt as to whether an intended posting or other conduct would violate HII policy, they should contact webmaster@hii-co.com.

To protect your privacy and the security of our workplace, we recommend following these safety tips*:

1. **Password care**: Make passwords long and strong; combine capital and lowercase letters with numbers and symbols to create a more secure password. Also, separate passwords for every account helps to thwart cybercriminals.
2. **Use caution when you click links you receive in messages from your friends on your social website**. Treat links in messages on these sites as you would links in e-mail messages. Also use caution when using shortened links.
3. **Know and manage your connections**: Accept connections from people you know, and use the social network’s privacy settings to control access to the information you share with them. Identity thieves may create fake profiles in order to get information from you.
4. **Keep personal information personal**: Be cautious about how much personal information you provide on social networking sites. The more information you post, the easier it may be for a hacker or someone else to use that information to steal your identity, access your data, or commit other crimes such as stalking.
5. **Search Your Own Name or Account**: To protect your reputation and ensure the security of your accounts, search your name or profiles from the perspective of a regular user in the application. This will let you know if there are other accounts in your name and will let you know what personal information others are able to see. Also, search your name using a search engine to discover if any false accounts are using your name or image.
6. **Don’t trust that a message really is from whom it says it’s from**. Hackers can break into accounts and send messages that look like they’re from your friends but aren’t. If you suspect a message is fraudulent, use an alternate method to contact your friend to find out. This includes invitations to join new social networks.
7. **To avoid giving away e-mail addresses of your friends, do not allow social networking services to scan your e-mail address book**. The site might use this information to send e-mail messages to everyone in your contact list or even everyone you’ve ever sent an e-mail message to with that e-mail address. Social networking sites should explain that they’re going to do this, but some do not.
8. **Be honest if you’re uncomfortable**. If a friend posts something about you that makes you uncomfortable or you think is inappropriate, let them know. Likewise, stay open-minded if a friend approaches you because something you’ve posted makes him or her uncomfortable. People have different tolerances for how much the world knows about them respect those differences.
9. **Take action**. If someone is harassing or threatening you, remove them from your friends list, block them, and report them to the site administrator.
10. **Type the address of your social networking site directly into your browser or use your personal bookmarks**. If you click a link to your site through e-mail or another website, you might be entering your account name and password into a fake site where your personal information could be stolen.
11. **Choose your social network carefully**. Evaluate the site you plan to use and make sure you understand the privacy policy. Find out if the site monitors content that people post. You will be providing personal
information to this website, so use the same criteria you would to select a site where you enter your credit card.

12. **Assume that everything you put on a social networking site is permanent.** Even if you delete your account, photos, videos and text may live on in screen shots or archives.

13. **Be careful about installing extras on your site.** Many social networking sites allow you to download third-party applications that let you do more with your personal page. Some of these may allow developers automatic access to public information and may access some private information. They may not be covered by the social network’s privacy policy. Criminals sometimes use these applications to steal your personal information. To download and use third-party applications safely, take the same safety precautions that you take with any other program or file you download from the Web.

14. **Stay aware of changes to a social network’s terms of service and privacy policy.**

15. **Consider disabling the geotagging features on social media profiles.** It announces to everyone in your social network where you are – information which you may not want to disclose. Also, don’t publicize vacation plans, especially dates you’ll be traveling.

16. **Due to the nature of our business, consider whether it’s prudent to disclose your job title and place of work in your social media profiles.** This is the type of information that may be used in phishing, a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures.

17. **If you do have access at work, use extra caution in all aspects to protect from security breaches or viruses.**

18. **If you have children:**
   a. Keep their profiles private so that only family and people you know see photos, important dates and other information.
   b. Make sure they’re not posting personal details, including phone numbers, home address, and the name of their school or Social Security number.
   c. Only allow them to publish photos and videos that don’t jeopardize their safety or their integrity.
   d. Make sure they choose a strong password that can’t be guessed, and that it gets changed every three months.
   e. Never allow them to accept friend requests from people they don’t know.
   f. Keep an open dialogue with your children. Ask them to let you know if they’ve received private messages from a stranger, or from someone at school who is teasing, harassing or threatening them. Those could be signs of cyber-bullying or even a sexual predator.

*Sources: Microsoft Corp., Privacy Rights Clearinghouse, StaySafeOnline.org, Norton Security, Kids.gov

Questions or concerns about these guidelines should be addressed to the HII Corporate Webmaster and Social Media Coordinator at: webmaster@hii-co.com

*Updated September 2017*