Huntington
Ingalls
Industries

Guidelines for Employee Use of Social Media

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

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

Employees should not access social media sites during their working hours. Outside of their working hours, employees may use social media through non-HII computer systems and networks. However, even when on social media, employees should remember that at HII, we are guided by our stated Values: Integrity, Safety, Honesty, Engagement and Responsibility. As such, all HII employees are expected to treat others with dignity and respect, and to communicate in a courteous and professional manner at all times – including on social media. If an HII employee posts or shares racist, sexist, bullying or other offensive content, it affects the workplace by potentially creating an intimidating, hostile, or offensive work environment. The consequences of such action may be disciplinary action, up to and including termination. Please refer to HII's Code of Ethics and Business Conduct for more 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.
- Do not use HII e-mail addresses to create social media profiles, and do not associate HII e-mail addresses with social media profiles.
- Do not use the same passwords for your HII login credentials and your social media profiles.
- Do not send or post on social media any 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 guidelines 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 values or policies, they should contact webmaster@hii-co.com.

Tips for Safeguarding Your Privacy and Protecting Your Family

- **Limit the amount of personal information you post**. Do not post information that would make you vulnerable, such as your address or information about your schedule or routine. If your connections post information about you, make sure the combined information is not more than you would be comfortable with strangers knowing. Also be considerate when posting information, including photos, about your connections.
- **Remember that the internet is a public resource**. Only post information you are comfortable with anyone seeing. This includes information and photos in your profile and in blogs and other forums. Also, once you post information online, it's impossible to retract. Even if you remove the information from a site, screen grabs, saved or cached versions may still exist.
- **Be wary of strangers.** The internet makes it easy for people to misrepresent their identities and motives. Consider limiting the people who are allowed to contact you on these sites. If you interact with people you do not know, be cautious about the amount of information you reveal or agreeing to meet them in person.
- **Be skeptical.** Don't believe everything you read online. People may post false or misleading information about various topics, including their own identities. Take appropriate precautions and try to verify the authenticity of any information before taking any action.
- **Evaluate your settings**. Take advantage of a site's privacy settings. The default settings for some sites may allow anyone to see your profile, but you may customize your settings to restrict access to only certain people. There is still a risk that some private information could be exposed despite these restrictions, so don't post anything that you wouldn't want the public to see. Sites may change their options periodically, so review your security and privacy settings regularly to make sure that your choices are still appropriate.
- **Be wary of third-party applications**. Third-party applications may provide entertainment or functionality in the forms of games, quizzes and polls, but use caution when deciding which applications to enable. Avoid applications that seem suspicious, and modify your settings to limit the amount of information the applications can access.
- **Use strong passwords**. Protect your account with passwords that cannot easily be guessed. If your password is compromised, someone else may be able to access your account and pretend to be you.
- **Check privacy policies**. Some sites may share information such as email addresses or user preferences with other companies. This may lead to an increase in spam. Also, try to locate the policy for handling referrals to make sure that you do not unintentionally sign your friends up for spam. Some sites will continue to send email messages to anyone you refer until they join.

- **Keep software — particularly your web browser — up to date**. Install software updates so that attackers cannot take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it.
- **Use and maintain anti-virus software**. Anti-virus software helps protect your computer against known viruses, so you may be able to detect and remove the virus before it can do any damage. Because attackers are continually writing new viruses, it is important to keep your definitions up to date.
- **Use two-factor authentication to prevent unauthorized logins.** Two-factor authentication or login verification via text message or other means can keep your accounts secure even if your username and password are stolen.
- **Avoid (and report) duplicate friend requests.** If you receive a request to connect with someone you know, but who you thought was already a friend or follower, double check your friends list before accepting the invitation. If the sender is already on your list, chances are good their account has been hacked.

Family Safety Tips for Using Social Media

- Insist that your children never give out personal information or plan a face-to-face meeting with anyone they meet online.
- Place the computer in a common area of your home to monitor use and enforce rules for when, how long, and in what way it can be used.
- Review your child's online profiles regularly. Remove any personal or identifying information.
- Review the profiles of your children's friends and the links that they are following.
- Remind your children that what you post on the internet stays there forever.
- Ensure your children use the most restrictive privacy settings available on the social networking sites where they have a personal profile.
- Encourage your children to tell an adult if they feel threatened by someone or feel uncomfortable because of something online.

Sources: Experian, Norton Security Online, Department of Homeland Security.

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

Updated Oct. 15, 2020