NEW YORK STATE | Military and Naval Affairs

KATHY HOCHUL
Governor
Commander-in-Chief

RAYMOND F. SHIELDS, JR.
Major General
The Adjutant General

MNAG-TAG

20 MAR 2024

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Division of Military and Naval Affairs' (DMNA) Cybersecurity Policy

1. References:

a. AR 25-2, Army Cybersecurity.

b. DoDI 8500.01, Cybersecurity.

2. Purpose. To provide leadership emphasis and individual responsibility for cybersecurity awareness and personal responsibility within the DMNA.

3. Applicability. This policy is applicable to all members assigned to the New York State's Organized Militia, including the New York Army National Guard, New York Air National Guard, New York Naval Militia, New York State Guard, all state, federal, and contract employees of the DMNA.

4. Guidance. Computer and information technology networks are essential to our professional and personal lives. It is a leadership and individual responsibility to protect information technology systems, networks, and data. The DMNA is committed to a culture that embraces information technology (IT) and Cybersecurity.

5. Security and professionalism must be embedded into everything our organization does; it is non-negotiable.

a. Small actions by a user can put the entire organization at risk, ranging from simple phishing all the way to full intrusions and data breach/loss. Leaders not only need to understand the dangers but also need to adjust the organizational culture to ensure a security focus. Users will need to embrace this, and in many ways incorporate it into their daily work and personal lives.

b. Social media is also an area that falls under the umbrella of Cyber Awareness. Many times, users have unintentionally provided information via social media that has had very negative impacts to the organization. You can mistakenly provide critical information that can cause disruptions to both personal and organizational readiness. Review your privacy settings, know your friends, and ensure you cautiously review location, timing, and information before clicking the post button.

c. Users are not permitted access to any Department of Defense (DoD) information system, unless in complete compliance with the DoD and Army personnel security requirements for operating in a SECRET (SIPRNet) or UNCLASSIFIED (NIPRNet) environment. Users must not directly access, download or view attachments containing or labeled as classified or unclassified sensitive information (i.e., Controlled Unclassified Information) from a device, equipment, system or network (i.e., cellphone, tablet, computer) not specifically authorized to process such information – either directly or through a website (i.e., webmail) – unless this is done in a formally authorized and secured manner (i.e., virtual environment, secure viewing application, sandbox application, secure thin client) that prevents such information from being either temporarily or permanently stored on the device, equipment, system, or network.

d. Users of government supplied devices or owners of personal devices used to gain access to information or services NOT approved for public release must use DoD or New York State Information Technology Services (NYS ITS) approved digital communication and storage methods using Common Access Card or other approved multi factor authentication methods. Authorized operators of NYS ITS systems or NYS web applications, must use those systems in accordance with all NYS approved policies and procedures.

e. Public Key is used to encrypt information and verify the origin of the sender of an email. It must be used to send sensitive information, information protected by the Privacy Act of 1974, and Information protected under the Health Insurance Portability and Accountability Act.

f. Misuse of systems or communication methods intentionally meant to disrupt operations or cause discourse, will not be tolerated. This includes actions such as "replying all" with jokes or unrelated information. This scenario can cause confusion, slow down network, and email services, and can potentially spread malicious files and or links if the original source is unknown. Do not reply all, ensure you double check the "To" and CC fields for intended recipients prior to sending emails, and avoid further contributing to these situations.

g. The user understands that Army IT resources will not be used in a manner that would reflect adversely on the Army, such as chain letters; unauthorized advertising, soliciting, or selling; uses involving gambling or pornography; uses that violate statute or regulation; or other uses that are incompatible with public service. The user understands that it is their duty to immediately report all cybersecurity related events, potential threats, vulnerabilities, and compromises or suspected compromises involving Army IT resources to the Information Systems Security Manager, in the MNCI-G6 Cybersecurity Office.

6. All personnel must develop automation competencies and an attitude of persistent education for IT systems and tools.

a. Information Technology systems, software and tools evolve exponentially. The reliance of all organization on them continues to expand; they are our day to day 'weapon system' that must be cared for and understood by each individual. Each user must embrace a learning attitude with their computer systems and understand each component to know its limitations and capabilities in order to effectively execute missions and routine responsibilities.

330 Old Niskayuna Road, Latham, New York 12110-3514 | 518-786-4500 | www.dmna.ny.gov

b. Leaders must push their subordinates to independently understand how to effectively use each aspect of the IT tools at their disposal. New technology or system updates should be seen as an opportunity to learn how to maximize that system. Users must become fully competent in navigating, using, and learning both current and future technology independently.

7. Completing the Annual Cyber Awareness course is one way to maintain an overview of cybersecurity threats and best practices to keep information and information systems secure. The training also reinforces best practices to keep the DoD and personal information and information systems secure, and stay abreast of changes in DoD cybersecurity policies. This will also keep users aligned with the Army IT User Agreement that is also signed annually. User accounts will not be issued/renewed without annual training and updated IT User Agreements.

8. Cybersecurity is a mechanism to ensure growth and the security of our organization. Everyone has a role in securing their part of cyberspace, including the devices and networks they use. Individual actions have a collective impact and when we use the internet safely, we make it more secure for everyone. We must all do our part by implementing stronger online security practices, raising community awareness, and educating our employees.

9. This policy is punitive in nature and violations may result in adverse administrative and disciplinary actions.

10. The primary point of contact for this policy is the Chief Information Officer/G6, COL Diane Armbruster at 518-786-4690, or via email at diane.m.armbruster.mil@army.mil.

RAYMOND F. SHIELDS, JR.
Major General, NYARNG
The Adjutant General

DISTRIBUTION:
AA, BB,
C, E,
F1-F8, S