DEPARTMENTS OF THE ARMY AND THE AIR FORCE
JOINT FORCE HEADQUARTERS - NEW YORK
330 OLD NISKAYUNA ROAD
LATHAM, NY 12110-3514

3 MAY 2021

MNAG-TAG

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: New York Army National Guard's (NYARNG) Cybersecurity Policy

1. References:

a. AR 25-2, memorandum (Army Cybersecurity), 04 April 2019.

b. DoDI 8500.01, (Cybersecurity), 14 March 2014.

2. Purpose. To provide leadership emphasis and individual responsibility for Cybersecurity awareness within the NYARNG.

3. Applicability. This policy applies to all state and federal employees of the Division of Military and Naval Affairs (DMNA), contractors and all members of the New York Army and Air National Guard, Naval Militia and New York Guard.

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 NYARNG is committed to a culture that embraces information technology (IT) and Cybersecurity.

5. Security 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, with those risks ranging from simple phishing all the way to full intrusions and data breach/loss. Leaders not only need to understand the dangers but adjust the organizational culture to ensure there is 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.

6. All personnel must develop automations 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.

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 and 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 Acceptable Use Policy that is also signed annually.

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

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

DISTRIBUTION:
AA,
BB
BR, C, D, E,
F1-F8