DEPARTMENTS OF THE ARMY AND AIR FORCE
JOINT FORCE HEADQUARTERS WISCONSIN
WISCONSIN NATIONAL GUARD
2400 WRIGHT STREET
POST OFFICE BOX 8111
MADISON WISCONSIN 53708-8111

WIJS/J6/SIT

14 August 2020

MEMORANDUM FOR The Department of Military Affairs

SUBJECT: Inappropriate Use of Government Owned Information and Communication Technologies – TAG POLICY MEMORANDUM 18

1. This policy applies to all users of government owned information and communications technology (ICT) systems and networks. The purpose of this policy is to define and prohibit inappropriate use of government technology resources in accordance with Title 5, Code of Federal Regulations part 2635, Standards of Ethical Conduct and DOD Regulation 5500.7-r, Joint Ethics Regulation, Sec 2-301, Department of Administration Information Technology Security Policy and State Statute 16.971.

2. The primary use of government ICT is for the conduct of official government business in a way that improves the efficiency and effectiveness between our internal users, and external customers and partners. ICT is a finite resource and efficient use must be stressed to obtain organizational effectiveness. Inappropriate use of ICT may result in system degradation or provide compromises to system security. Therefore, inappropriate use of enterprise ICT may be the basis for consideration of disciplinary action against military and civilian employees or cause for contractor dismissal.

3. For purposes of this policy letter, ICT includes but is not limited to computers, mobile electronic devices, radios, printers, conference bridges, web or desktop based collaboration platforms, video teleconference systems, televisions, DVD players, faxes, scanners, tablets, phones and copiers.

4. Commanders and supervisors, at all levels, must make anyone using various ICT systems and networks aware of permissible and unauthorized uses of those systems. In general, it is unacceptable for a Department of Military Affairs/Wisconsin National Guard (DMA/WING) user to access, use, submit, publish, display, or transmit on any government network or system any information which:

a. Violates or infringes on the rights of any other person, including the right to privacy.

b. Contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive; or otherwise biased, discriminatory, or illegal material.

c. Violates military or state regulations or policies prohibiting sexual harassment or harassment based on a protected status.

d. Encourages the use of controlled substances or uses the system for the purpose of criminal intent.

e. Is used for any political activity, political fundraising or to promote or advocate for a particular political candidate, position or policy.

f. Uses the system for any other illegal purpose, private fund raising or commercial activity.

5. Email is a pervasive component of our daily operations. Email users must use email resources responsibly and abide by normal standards of professional and personal courtesy and conduct. Email, as with any ICT, will not be used in a way which:

a. Interferes with official duties, undermines readiness or reflects adversely upon the organization (such as uses involving pornography, unofficial advertising or soliciting).

b. Interferes with others' use of email or email systems such as broadcasting unsubstantiated rumors, chain letters, warnings or spam.

c. Causes unneeded, additional traffic that degrades other users productivity (sending large attachments versus links; inappropriate or organization-wide announcements, resending information already transmitted, etc).

6. Voice telecommunications is another key component of the organizations capabilities and is subject to the same usage considerations as other ICTs. While voice systems lack capability to move information, usage entails a system and fiscal cost. Therefore, voice systems are only used for official business that is necessary and of interest to the government.

a. Users that have access to four or six digit dialing (on–net calls) should do so at all times.

b. Defense Switched Network (DSN) is the principal long distance voice communications network for the Department of Defense (DOD) and must be a user's first choice for long distance voice communications and faxes. Only official calls are permitted using the DSN system.

7. Classified Communications. Most state and federal government communications systems are not secure. DMA/WING employees will not transmit classified information over any communication system unless it is transmitted using approved security procedures and practices (e.g. from secure networks and workstations protected with encryption). DMA/WING employees should exercise extreme care when transmitting any sensitive information, personally identifiable information, or other valued data. Information transmitted over an open network (such as through unsecured fax or telephone) may be accessible to anyone else on the network.

8. By using government ICT, users give consent to monitoring. Electronic files, voice mails, logs and email sent and received are the property of the organization, not the employee. Users are potentially liable for costs incurred by inappropriate use of ICT. Reimbursement to the government may include additional administrative processing fees.

9. Users must always be cognizant of ICT risks with regards to information security and operational security (OPSEC). ICT has become a ubiquitous part of our society. Lines that divide connectivity and ITC capabilities used in professional work assignments blur with those of personal capabilities, posing risks and lowering barriers to rapid and widespread information sharing. However, employees may use government ICT for occasional and incidental personal communications. Employees must bear in mind operational security and information security when using ICT for personal use. Users must ensure that personal communications:

a. Do not interfere with the organization's operation or performance of official duties.

b. Are conducted after duty hours, on breaks or on non-government devices and systems, when reasonable.

c. Do not degrade the performance of enterprise information systems.

d. Do not create additional expense to the government (i.e. strive to use calling cards and toll free numbers for long distance calls for calling entities external to the WING or DMA). Long distance calls into the Wisconsin Army and Air National Guard entities do create a cost to the hosting agency.

10. Users may submit complaints about inappropriate ICT to their respective supervisors or information management office. If inappropriate use is substantiated, organizational ICT management personnel will inform the employee's commander/supervisor to consider appropriate disciplinary or other corrective action. Substantiated claims may also be referred to the judge advocate or state legal counsel for further review.

PAUL E. KNAPP
Maj Gen, Wisconsin National Guard
The Adjutant General