Electronic Messaging Policy
USG Policy 6 (1.10) | Approved by the Executive Director, May 2019

I. Purpose and Applicability

This policy outlines expectations for appropriate, safe, and effective electronic messaging use. This policy will help USG reduce the risk of an electronic messaging-related security incident, foster good business communications both internal and external to USG, and provide consistent and professional application of USG's electronic messaging principles.

The scope of this policy includes all individual work electronic messaging accounts, shared work electronic messaging accounts, and mass electronic messaging applications and services purchased by USG and used by USG's personnel regardless of ownership of computer system or device. It also covers all electronic messages sent and received from USG owned or leased computer systems and devices, as well as personal use electronic messaging accounts accessed over USG's network.

All individual or shared work electronic messaging accounts used by USG personnel is hereinafter referred to as "USG associated accounts". The Universities at Shady Grove is hereinafter referred to as "USG" and the Office of Information Technology as "OIT." This policy will be reviewed annually to ensure continual compliance with USM IT Security Standards and other pertinent policies, laws and industry standards.

II. Definitions

A. *Auto Responder*: an electronic messages function that sends a predetermined response to anyone who sends an electronic message to a certain address. Often used by employees who will not have access to electronic messages for an extended period of time, to notify senders of their absence.

B. *Certificate*: also called a "Digital Certificate." A file that confirms the identity of an entity, such as a USG or person. Often used in VPN and encryption management to establish trust of the remote entity.

C. *Data Leakage:* also called Data Loss, data leakage refers to data or intellectual property that is pilfered in small amounts or otherwise removed from the network or computer systems. Data leakage is sometimes malicious and sometimes inadvertent by users with good intentions.

D. *Electronic messages*: electronic messages refer to all electronic messaging applications and services, including but not limited to, e-mail and instant messaging.

E. *Encryption*: the process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored.

F. *Mobile Device*: a portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.

G. *Password*: a sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Also known as a passphrase or passcode.

H. *Spam*: unsolicited bulk electronic messages. Spam often includes advertisements, but can include malware, links to infected websites, or other malicious or objectionable content.

I. *Smartphone*: a mobile telephone that offers additional applications, such as PDA functions and electronic messages.

J. *Two Factor Authentication*: a means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

III. Guidelines for Electronic Messaging Accounts

Users are asked to exercise common sense when sending or receiving electronic messaging from USG associated accounts. Additionally, the following applies to the proper use of the USG associated accounts.

A. Sending Electronic messaging

When using a USG associated electronic messaging account, electronic messaging must be addressed and sent carefully. Users should keep in mind that USG loses any control of electronic messaging once it is sent. Users must take extreme care when typing in addresses, particularly when electronic messaging address auto-complete features are enabled; using the "reply all" function; or using distribution lists in order to avoid inadvertent information disclosure to an unintended recipient. Careful use of electronic messaging will help USG avoid the unintentional disclosure of sensitive or non-public information as defined in the USG Data Classification Policy 6 (2.10).

B. Electronic Messaging Signature

Electronic messaging signatures (contact information appended to the bottom of each outgoing electronic message) may or may not be used, at the discretion of the individual user. Users are asked to keep any electronic messaging signatures professional in nature; however, USG does not place any restrictions on electronic messaging signature content.

C. Auto-Responders

USG neither requires nor forbids the use of electronic messaging auto-responders.

D. Mass Electronic Messaging

USG makes the distinction between the sending of mass electronic messages and the sending of unsolicited electronic messages (spam). Mass electronic messages may be useful for both marketing and non-marketing purposes, such as when communicating with USG's employees or other campus populations regarding internal activities or service disruptions, and is allowed as the situation dictates. The sending of spam, on the other hand, is strictly prohibited.

It is USG's intention to comply with applicable laws governing the sending of mass electronic messages. In order to be consistent with good business practices, USG requires that electronic messaging sent to more than twenty (20) recipients external to USG have the following characteristics, when applicable based on messaging method:

1. Electronic messages must contain instructions on how to unsubscribe from receiving future electronic messages, if applicable. Unsubscribe requests must be honored immediately.
2. Electronic messages must contain a subject line relevant to the content.
3. Electronic messages must contain contact information, including the full physical address, of the sender.
4. Electronic messages must contain no intentionally misleading information (including the electronic messaging header), blind redirects, or deceptive links.

Note that electronic messages sent to USG employees, existing partners, or persons who have already inquired about USG's services are exempt from the above requirements.

E. Electronic Messaging Attachments and Links

Users must use care when opening electronic message attachments. Viruses, Trojans, and other malware can be easily delivered as an electronic message attachment. Users should:

1. Never open unexpected electronic message attachments.
2. Never open electronic message attachments from unknown sources.
3. Never click links within electronic messages unless he or she is certain of the link's safety. It is often best to copy and paste the link into your web browser, or retype the URL, as specially formatted electronic messages can hide a malicious URL.

USG reserves the right to use methods to block what it considers to be dangerous electronic messages or strip potentially harmful electronic message attachments as it deems necessary.

F. Monitoring and Privacy

Users should expect no privacy when using USG’s network or USG resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. USG reserves the right to monitor any and all use of the computer network. To ensure compliance with USG policies this may include the interception and review of any electronic messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

G. Ownership of Electronic Messages

Users should be advised that USG owns and maintains all legal rights to its USG associated accounts and mass electronic messaging systems, and thus any electronic messages passing through these accounts and systems is owned by USG. Therefore, all electronic messages may be subject to review by authorized USG staff for purposes not originally intended by the user. Keep in mind that electronic messaging may be backed up, otherwise copied, retained, or used for legal, disciplinary, or other reasons. Additionally, the user should be advised that electronic messages sent to or from certain public or governmental entities may be considered public record.

H. Contents of Received Electronic Messages

Users must understand that USG has little control over the contents of inbound electronic messages, and that electronic messages may contain material that the user finds offensive. If unsolicited electronic messages become a problem, USG may attempt to reduce the number of these electronic messages that the users receive, however no solution will be 100% effective. The best course of action is to not open electronic messages that, in the user's opinion, seem suspicious. If the user is particularly concerned about an electronic message, or believes that it contains illegal content, he or she should notify his or her supervisor.

I. Access to Electronic Messages from Mobile Phones

Many mobile devices, such as smartphones or tablets, provide the capability to send and receive electronic messages. USG permits users to access USG associated accounts from mobile devices. Refer to USG's Mobile Device Policy 6 (1.40) for more information.

IV. External and/or Personal Electronic Messaging Accounts

USG recognizes that users may have personal electronic messaging accounts in addition to their USG associated accounts. The following sections apply to non-USG associated electronic messaging accounts:

A. Use for USG Business

Users must use their USG associated accounts for all business-related electronic messages. Users are prohibited from sending business electronic messages from personal electronic messaging accounts.

B. Access from the USG Network

Users are permitted to access external or personal electronic messaging accounts from the USG network, as long as such access uses no more than a trivial amount of the users' time and USG resources.

C. Use for Personal Reasons

Users are strongly encouraged to use a personal electronic messaging account for any non-business communication. Users must follow applicable policies regarding the access of personal electronic messaging accounts from the USG network.

V. Confidential Data and Electronic Messages

The following sections relate to confidential data and electronic messages:

A. Passwords

As with any USG passwords, passwords used to access electronic messaging accounts must be kept confidential and used in adherence with USG’s Password Policy 6 (3.40). At the discretion of OIT, USG may further secure electronic messages with certificates, two-factor authentication, or other security mechanisms.

B. Electronic Messaging Confidential Data

Electronic messaging is an insecure means of communication. Users should think of electronic messages as they would a postcard, which, like electronic messages, can be intercepted and read on the way to its intended recipient. USG requires that any electronic messages containing confidential information, regardless of whether the recipient is internal or external to the USG network must be encrypted in accordance with USG’s Confidential Data Policy 6 (2.00) and Encryption Policy 6 (2.30).

VI. Electronic Messaging Administration

USG will use its best effort to administer USG associated accounts in a manner that allows the user to both be productive while working as well as reduce the risk of an electronic message-related security incident.

A. Filtering of Electronic Messages

A good way to mitigate risk from electronic messages is to filter it before it reaches the user so that the user receives only safe, business-related messages. At this time, USG does not wish to filter electronic messages at the gateway or electronic messaging server for spam or viruses; however, it reserves the right to do so at any time. Additionally, many electronic messaging and/or anti-malware programs will identify and quarantine electronic messages that it deems suspicious. This functionality may or may not be used at the discretion of OIT.

B. Electronic Message Disclaimers

The use of an electronic message disclaimer, usually as text appended to the end of every outgoing electronic message, is often recommended as an additional component of a USG's risk reduction efforts. At this time USG does not require the use of electronic message disclaimers.

C. Electronic Messages Deletion

Users are encouraged to delete electronic messages periodically when the electronic message is no longer needed for business purposes. The goal of this policy is to keep the size of the user's electronic messaging account manageable, and reduce the burden to store and backup unnecessary electronic messages. However, users are strictly forbidden from deleting electronic messages in an attempt to hide a violation of this or another USG policy. Further, electronic messages must not be deleted when there is an active investigation or litigation where that electronic message may be relevant.

D. Retention and Backup

Electronic messages should be retained and backed up in accordance with the applicable policies, which may include but are not limited to USG's Data Classification Policy 6 (2.10), Confidential Data Policy 6 (2.00), Backup Policy 6 (3.00), and Data Retention Policy 6 (2.40).

E. Electronic Messaging Aliases

Often the use of an electronic messaging alias, which is a generic address that forwards electronic messages to a user's account or group of users, is a good idea when the electronic messaging address needs to be in the public domain, such as on the Internet. Aliases reduce the exposure of unnecessary information, such as the address format for USG electronic messages, as well as (often) the names of USG employees who handle certain functions. Keeping this information private can decrease risk by reducing the chances of a social engineering attack.

F. Account Activation

Individual USG associated accounts will be set up for each user determined to have a legitimate business need to send and receive electronic messages. Accounts will be set up at the time a new hire starts with USG, or when a promotion or change in work responsibilities for an existing employee creates the need to send and receive electronic messages. Electronic messaging accounts may be given to non-employees, contractors, or other individuals authorized to conduct certain aspects of USG's business.

G. Account Termination

When a user leaves the USG, or his or her electronic messaging account access is officially terminated for another reason, USG will disable the user's access to the account by password change, disabling the account, or another method. USG is under no obligation to block the account from receiving electronic messages, and may continue to forward inbound electronic messages sent to that account to another user, or set up an auto-response to notify the sender that the user is no longer employed by USG.

VII. Prohibited Actions

A. The following actions shall constitute unacceptable use of USG associated accounts. This list is not exhaustive, but provides a frame of reference for types of activities that are deemed unacceptable. The user may not use USG associated accounts to:

1. Send any information that is illegal under applicable laws.
2. Access another user's electronic messaging account without a) the knowledge or permission of that user - which should only occur in extreme circumstances, b) the approval of USG executives in the case of an investigation, or c) when such access constitutes a function of the employee's normal job responsibilities.
3. Send any electronic messages that may cause embarrassment, damage to reputation, or other harm to USG.

4. Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, harassing, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
5. Send electronic messages that cause disruption to the workplace environment or create a hostile workplace. This includes sending electronic messages that are intentionally inflammatory, or that include information not conducive to a professional working atmosphere.
6. Make fraudulent offers for products or services.
7. Attempt to impersonate another person or forge an electronic messages header.
8. Send spam, solicitations, chain letters, or pyramid schemes.
9. Knowingly misrepresent USG's capabilities, business practices, warranties, pricing, or policies.
10. Conduct non-USG-related business.

USG may take steps to report and prosecute violations of this policy, in accordance with USG standards and applicable laws.

B. Data Leakage
Data can leave the network in a number of ways. Often this occurs unintentionally by a user with good intentions. For this reason, electronic messages pose a particular challenge to USG's control of its data.

Unauthorized electronic messaging of USG data, confidential or otherwise, to external electronic messaging accounts for the purpose of saving this data external to USG systems is prohibited. If a user needs access to information from external systems (such as from home or while traveling), that user should notify his or her supervisor rather than electronic messaging the data to a personal account or otherwise removing it from USG systems. USG may employ data loss prevention techniques to protect against leakage of confidential data at the discretion of OIT.

VIII. Enforcement

A. The enforcement of this policy will be carried out by authorized USG OIT personnel designated by the Director of OIT and USG Senior Leadership. Violations may result in disciplinary actions, which may include suspension, restriction, or revocation of access. Where illegal activities or theft of USG property (physical or intellectual) are suspected, USG may report such activities to the state/federal law enforcement authorities.

IX. Revision History

Date	Description	Revised By
08/22/2018	Initial Policy Creation	Russell Schlosburg

X. Related Documents

A. USM IT Security Standards v4
http://www.usmd.edu/usm/adminfinance/itcc/USMITSecurityStandards.pdf