SECURITY CONSIDERATIONS

Division of IT | 202-994-4948 | ithelp@gwu.edu | IT.GWU.EDU

1 **PHISHING** A type of online scam that uses false emails, forms and websites to trick a person into providing personal information. This can include usernames, passwords, Social Security numbers, credit cards and other personal information. If you believe that you have received a phishing message, please report it to abuse@gwu.edu. Your report will play a key role in helping others at GW avoid similar scams. Two good rules to follow: don't open any email attachment you were not expecting and and don't log in to any websites you visit through email. Visit IT.GWU.EDU/security to watch videos on how to avoid a phishing attempt.

2 **KNOW YOUR DATA** To best secure data in your possession, you must first know what you have and how sensitive it is. Know your data, a key component of the Information Security Policy, requires each person to understand the data classification guidelines and apply it to the way that data is handled and secured through its lifecycle. Regulated data, which is the highest criticality data possible under the data classification guideline, may only be stored and transmitted in certain, pre-approved methods. For more information on how you can classify and know you data, visit the University Compliance and Privacy Information Management website compliance.gwu.edu.

3 **ENCRYPT** Encryption is one of the most effective controls for securing the privacy and confidentiality of data. Whether at rest or in transit, encryption technology protects our non-public data. Three ways that you can implement encryption are full-disk encryption, secure transmission by using "https" when online and email encryption. Full-disk encryption protects the contents of the hard drive in your computer or portable media such as DVDs and portable hard disk drives. If your computer is ever lost or stolen, the thief will not be able to access the contents of your drive without the decryption key. When submitting information via web forms, always ensure that the application uses "https" instead of "http". The "s" means your form submittal and the transmission is encrypted in transit. Sign up for our email encryption service to help protect restricted data and private conversations between you and non-GW personnel.

4 **TRUSTWORTHY SOFTWARE** All software can be vulnerable to attack and exploitation by criminals. To reduce the risk of these attacks, it is important that all software be routinely updated. This includes your operating system (Mac OS, Windows), web browser (Chrome, Firefox, Safari), and other applications such as Adobe Acrobat, Flash and Microsoft Silverlight. In addition to updating your software regularly, make sure that you only download software from legitimate sources. Some websites may advertise cheap or free software but beware - some of this software may have been altered to run malicious code alongside the legitimate application. On GW owned and managed equipment, some updates are automatically installed.

5 **SAFE BROWSING** The Internet is the greatest tool that humans have ever created but unfortunately it is also an incredibly useful tool for criminals. Avoiding web-based attacks requires vigilance. Ad blockers can help reduce the risk of "malvertising" or malicious code hidden in advertising. Taking care in typing website addresses is also important. Attackers often buy domain names that are incorrect spellings of popular websites to victimize people who incorrectly type a website address. Finally, using anti-virus software such as Symantec Endpoint Protection can help mitigate the threat of known malware encountered during browsing the web.

GW | Division of Information Technology