UMW Information Technology Security Program

Annual Security Awareness Training for

UMW Faculty and Staff

ANNUAL SECURITY AWARENESS TRAINING – 2012

Network and Computer Use Policy

Users of information technology resources at the University of Mary Washington must use these resources responsibly and in compliance with the Network and Computer Use Policy. Using University-owned computers, networks, or other information technology resources constitutes acknowledgment that the user understands and commits to compliance with the University's Network and Computer Use Policy and related policies and procedures.

Network and Computer Use Policy

The complete policy and user responsibilities may be viewed on the Policies Section of the UMW website.

Other Information Security Related Policies

There are a number of other Information Security policies that users should be aware of. Links to important policies that you should be aware of are on this slide.

- Information Technology Security Program Policy
- Administrative Data Access Policy
- Electronic Storage of Highly Sensitive Data Policy
- Identity Management Credentials Policy
- Other important information security policies, standards and procedures

Encryption Protection and Data Disposal

- For encryption protection, reference the following standard: http://technology.umw.edu/it-policies/data-encryption-standard/
- For electronic data disposal, reference the following policy: http://technology.umw.edu/it-policies/electronic-data-removal-procedure/

UMW Data Classification Standard

The university has defined three levels of data classification for enterprise data. All enterprise data fall into one of these categories:

- Public Data
- Protected Data
- Highly Sensitive Data

UMW Data Classification Standard: Public Data

General administrative data that are intentionally made public are classified as not sensitive and defined as 'Public Data'. This includes all general administrative data that are not legally restricted or judged by data stewards to be limited access data. Examples of UMW public data include digital editions of such publications as the institution's Statistical Profile and the President's Annual Report of Gifts. The Schedule of Course Offerings, published each semester, along with the university's online PeopleSearch Directory serve as other examples of public data.

UMW Data Classification Standard: Public Data

Public data access does not require personal authentication credentials.

UMW Data Classification Standard: Highly Sensitive Data

The following data is classified as Highly Sensitive Data:

Personally identifiable information including: SSNs, Passport Numbers, Drivers License Numbers, financial account numbers (credit card numbers, debit card numbers, banking account numbers), and full name in conjunction with corresponding full date of birth.

UMW Data Classification Standard: Highly Sensitive Data

Access to Highly Sensitive Data may only be authorized by Data Stewards and Data Security Contacts, as defined in the Administrative Data Access Policy, and requires the completion of the University of Mary Washington Administrative Data User Account Request Form.

Securing Highly Sensitive Data

Highly Sensitive Data must not be stored or kept on any non-network storage device or media. Prohibited storage media includes storage on desktop computers, laptop computers, PDAs, cell phones, USB drives, thumb drives, memory cards, CDs, DVDs, local external hard drives and other USB devices.

Highly Sensitive Data should not be distributed via reports, spreadsheets, emails or email attachments.

UMW Data Classification Standard: Protected Data

By default, all administrative data that is not explicitly defined as Highly Sensitive Data, or is not intended to be made publicly available, is classified as Protected Data. For example, FERPA protected data not covered under the definition of "Highly Sensitive" is classified as "Protected".

Access to Protected Data is authorized by data stewards and data security contacts as described in the Administrative Data Access Policy and requires the completion of the University of Mary Washington Administrative Data User Account Request Form.

UMW Data Classification Standard: Protected Data

Secure credentials are required to access protected university data.

Standards or guidelines governing the release, distribution and dissemination of protected data by individuals authorized to access it is controlled and administered by the designated Data Stewards.

UMW Data Classification Standard

	Definition	Access	Secure Credentials	Example	Other
Public	General administrative data	Unrestricted	No	Report of Annual Gifts	
Highly Sensitive	Personally identifiable information.	Restricted	Yes	SSNs, credit card numbers	May only be stored on a network drive.
Protected Data	Data that isn't publically available, but that isn't highly sensitive.	Restricted	Yes	Student addresses	

PHISHING

Phishing is a cyber crime where well designed and legitimate looking emails and pop up messages lure victims into revealing their username, password, credit card number, Social Security number, or other sensitive information. Even though the problem is not new, there never seems to be a shortage of victims.

PHISHING

Phishing messages appear to be authentic and often mimic the type of communication you would expect to receive from trusted organizations, such as banks, merchants, or university system administrators. You should never trust email or pop up messages that ask you to confirm, validate, or update your information by responding to the email or by following a link.

PHISHING

The UMW IT Help Desk and system administrators will never send you an email requesting you to validate, confirm or update your account passwords or other personal information.

Reporting a Security Incident

If you fall victim to a phishing scam, believe that your UMW account credentials have been compromised, or have reason to believe that UMW IT system protocols, policies or procedures have been violated, you should immediately:

1. Change your password, and
2. Report the incident by sending an email to it-abuse@umw.edu or contacting UMW's ISO at rusler@umw.edu.

Reporting a Security Incident

Additional information about reporting security incidents, or about information security in general, may be found at the IT Information Security website.

Protect Your Passwords

There are a number of steps that you can take to protect your passwords. These tips apply to the passwords that you have for the UMW systems, as well as for other systems. Some of these tips are:

- Never share your passwords with anyone. Your password verifies your identity as an authorized user. You will be held responsible for misuse of your account if your password is shared with others.

Protect Your Passwords

- Choose a strong password that is hard to guess.
- Passwords should never be dictionary words or names. More secure passwords are those which are based on pass phrases.

Protect Your Passwords

- Don't record or leave passwords where others can find them. Remembering multiple passwords can be challenging, especially if they have to be changed regularly. This often results in passwords being written down, often in inappropriate locations, like under a keyboard or taped to a computer screen. Password Safe is free open-source software you can use to securely store your passwords.

Protect Your Passwords

- Never provide your password in an email or in a response to an email request. Please know that UMW IT personnel will never ask for your password.
- Use different passwords for different websites and services. Do not use your UMW account credentials on other, non-UMW, systems and applications.
- Use passwords that are easy for you to remember and difficult for others to guess. Again, passwords should not be dictionary words or names, more secure passwords are those which are based on pass phrases.

Protect Your Passwords

- Change passwords immediately if they have been compromised. Contact it-abuse@umw.edu or the University's ISO if it has been compromised.
- Change passwords frequently. UMW requires that passwords be changed every 90 days.
- Be careful about where passwords are saved on computers. Some software dialog boxes present an option to save or remember a password. Selecting this option poses a potential security risk. It is best to never save passwords in dialog boxes.

Identity Theft

Don't give out UMW or personal information on the phone, through the mail or over the Internet (through email or online forms, or any other manner) unless you have initiated the contact or are sure you know who you're dealing with. Identity thieves may pose as representatives of banks, credit card companies and even government agencies to get you to reveal your SSN, mother's maiden name, account numbers and other identifying information.

Identity Theft

Before you share any highly sensitive or protected information, confirm that you are dealing with a legitimate organization.

Lock your computer

To help protect the information accessible from your computer, you should lock it when you are away from your desk. Manually locking your computer (Ctrl-Alt-Del on a Windows computer) or setting a password-protected screen saver, offer a layer of protection by preventing others from seeing your screen or using your computer when you are away from your desk.

Security Awareness

Most breaches and compromises of sensitive data can be prevented by security awareness and good security habits. All UMW employees are required to complete security awareness training.

Security Awareness

Employees responsible for administering or supporting central UMW IT systems, or for authorizing access to sensitive data, will be required to attend additional security awareness training. University employee security awareness training requirements are outlined in the Security Awareness Education Standard.

Responsibility

Our Shared Responsibility means each of us must do our part. If each of us does, together we will be more resistant and resilient, protecting ourselves and our university.

Now that you have completed the 2012 Annual Security Awareness Training, please click on the Quiz button and complete the 4-item quiz that is located in Canvas. You must score 100% on the quiz to satisfy this requirement.

ANNUAL SECURITY AWARENESS TRAINING – 2012