Georgia Southern University
Digital Commons@Georgia Southern

Information Security Newsletter

Information Security Newsletter

Issue 4, October 27, 2014

Follow this and additional works at: https://digitalcommons.georgiasouthern.edu/infosecnews

Part of the Computer Sciences Commons, and the Higher Education Commons

Recommended Citation
"Information Security Newsletter" (2014). *Information Security Newsletter*. 4.
https://digitalcommons.georgiasouthern.edu/infosecnews/4

This newsletter is brought to you for free and open access by Digital Commons@Georgia Southern. It has been accepted for inclusion in Information Security Newsletter by an authorized administrator of Digital Commons@Georgia Southern. For more information, please contact digitalcommons@georgiasouthern.edu.

Information Security Newsletter

Information Security Office
Georgia Southern University

10/27/2014

2014/4

Policies, Standards and Guidelines

We often hear about "policies", "standards", and "guidelines", but what are they and why do we need them?

To start with let's define them.

"A **policy is typically a document that outlines requirements or rules that must be met. Policies are usually point-specific, covering a single area. For example, an "Acceptable Use" policy would cover the rules and regulations for appropriate use of the computing facilities.*

*A **standard** is typically collections of system-specific or procedural-specific requirements that must be met by everyone. For example, you might have a standard that describes how to secure a workstation for use on the network. People must follow this standard exactly if they wish to use a workstation on campus network.*

*A **guideline** is typically a collection of system specific or procedural specific "suggestions" for best practice. They are not requirements to be met, but are strongly recommended.*

Effective policies make frequent references to standards and guidelines that exist within an organization."

**http://www.sans.org/security-resources/policies*

What's the process for defining, creating, approving and reviewing policies? The document IT Policy Development & Review Process will define it for you.

Why do we need them?
The University's business requires that a lot of important information be utilized to fulfill its mission of teaching, scholarship, research and service. To that end there are many Federal, state and local regulations and laws that require policies and standards for protection of the information the University works with. The policies and standards also help protect the university and its employees.

Good policies and standards also give direction. They help us to know what is expected

National Cyber Security Awareness Month

Weekly Themes: InfoSec will focus on a different cyber security issue for each week in October.

Week 1 October 6-10
Theme: General online safety and STOP. THINK. CONNECT.

Week 2 October 13-17
Theme: Social Media – How to stay safe and still be friendly.

Week 3: October 20-24
Theme: Mobile Security – Protecting information on the go.

Week 4: October 27-31
Theme: University Policies that strengthen our Cyber security posture

More information can be found at:

www.Staysafeonline.org

of us and they can direct us in how to meet those expectations.

IT Services has a number of policies and standards that have been in place for some time. Recently many of those policies have been updated. New policies have also been approved. The following short list contains some of the newer policies and the link to all IT Services policies and standards.

IT Remote Access policy: *This policy defines remote access and the associated risks. It contains appropriate controls and protections required to mitigate these risks to preserve and protect University IT assets.*

Password Standard: *This document defines the standards for creating, maintaining and securing passwords at Georgia Southern University.*

university resources or houses university data.

Telecommunications Policy: *Defines the allowed and prohibited use of all State telephone services.*

Protection and Security of Records Policy: *This document defines that all users of the university have a responsibility to protect those assets from unauthorized access, destruction, disclosure,*

December 31st is the last day to complete your Cyber Security Awareness Training in BuildingABetterU. For instructions, visit

http://its.georgiasouthern.edu/infosec/cyber-security-awareness-course-instructions/

IT Acceptable Use Policy: *This document defines acceptable technology and information use practices, promotes an understanding of responsible use of university IT resources, and seeks to protect the University's IT resources, and preserves the relevant policies, regulations and laws.*

HEOA P2P Compliance Plan: *This document outlines the need for compliance with the Higher Education Opportunity Act (HEOA) and the procedures used to "combat the unauthorized distribution of copyrighted material by users of the institution's network, without unduly interfering with educational and research use of the network".*

Workstation Security Standards: *This document defines the configuration, maintenance and securing of Georgia Southern workstations. This standard applies to all university owned computers or computers that are used for Georgia Southern business.*

Workstation Management Standards: *This documents how technical support is to manage university owned workstations. It defines how workstations are accessed remotely and defines the limits to this kind of access.*

Server Security Standards: *This document defines how to configure, maintain and secure any Georgia Southern University server or any sever that utilizes*

generation, modification or transmission; and are expected to be familiar with and comply with University System procedures for protection and security of records.

Data Stewardship and classification standard: *This document defines who is responsible for the University's data, defines information in classes to help understand what information can be disclosed and how to protect the confidentiality, integrity and availability of University information.*

Campus Firewall Policy: *This defines who implements and maintains university owned technology firewalls.*

For all of IT Services' policies and standards go to:

https://inside.georgiasouthern.edu/President/Policy/Published%20Policies/Forms/AllItems.aspx

The Office of Information Security promotes a secure environment for the university to meet its mission of academic distinction in teaching, scholarship, research, and service.

Michael Fox, Chief Information Security Officer, Georgia Southern University

Email: security@georgiasouthern.edu Web: GeorgiaSouthern.edu/infosec