信息-risk安全新闻

信息-risk安全办公室
乔治亚南部大学

10月27日2014年

每周主题：信息安全

10月6日至10日
主题：一般在线安全

10月13日至17日
主题：社交媒体——如何保持安全同时保持友好。

10月20日至24日
主题：移动安全——保护在移动中的信息。

10月27日至31日
主题：大学政策加强我们的网络安全。

更多信息可以找到：
www.Staysafeonline.org

政策、标准和指南

我们经常听到“政策”、“标准”和“指南”，但它们是什么以及为什么我们需要它们？

让我们先定义它们。

*“政策”通常是概述必须满足的规则或要求的文件。政策通常是点对点的，覆盖一个单一的领域。例如，“可接受使用”政策会概述使用计算设施的规则和规定。

*“标准”通常是系统特定或程序特定的要求的集合，必须由每个人遵守。例如，你可能有一个标准描述如何在校园网络上保护工作站。人们必须严格遵守此标准。

*“指南”通常是一套系统特定或程序特定的“建议”最佳实践。它们不是必须满足的要求，但强烈推荐。

政策、标准和指南

有应用程序使用的规则和规定。

标准是系统特定或程序特定的要求的集合，必须由每个人遵守。例如，你可能有一个标准描述如何在校园网络上保护工作站。人们必须严格遵守此标准。

指南是一套系统特定或程序特定的“建议”最佳实践。

为什么我们需要它们？

大学的业务需要大量重要信息来履行其教学、研究、奖学金和服务机构的使命。

好的政策和标准也能提供方向。它们帮助我们了解期望。

最新的定义，创建，批准和审核政策的文档IT政策开发和审查过程将定义它

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

**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.

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

**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.

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

**Workstation Management Standards:** This document 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.

**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.

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

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

https://inside.georgiasouthern.edu/President/Policy/PublishedPolicies/Forms/AllItems.aspx