

# Information Technology Policies

## Working Paper

Scott Woodison  
IT Audit Manager  
BOR



1 October 2002

# DRAFT

Version 1.0

## **Purpose of this paper**

The purpose of this brief paper is to provide some basic information that can be used to develop Information Technology (IT) policies for the institutions of the USG. The topic of IT Policies is a broad one and this paper is only designed to present enough information to help the user get started on developing their own policies, tailored to their institution. .

This paper provides a skeleton or structure and some suggested areas that will require policies, standards and procedures. References and resources are listed at the end.

## **Need for Policies**

Well thought out and documented policies are required for the smooth functioning of a successful IT organization. Without defined policies, and the resulting standards and procedures, it is extremely difficult manage and direct an IT organization.

These policies also must be based on a complete risk analysis. It is imperative that we protect critical systems. However, we can overprotect a system. We do not want to put a \$100 lock on an asset with a \$5 value. A risk analysis will allow the user to develop the proper policies, standards and procedures.

## **Board of Regents Security Policy requirements**

The Board of Regents has set out their requirements for IT security policies and training in the Board of Regents Policy Manual, Finance and Business section 700. It states in part:

### 712 COMPUTER SECURITY POLICY

#### 712.01 GENERAL POLICY

The Board of Regents recognizes that all computer and computer related resources are valuable state assets and require some degree of protection. The degree of protection needed is based on the nature of the resource and its intended use. The Board also recognizes that, while no security procedures will provide for absolute security, all institutions of the System have the responsibility to minimize risk by enacting a computer security or related policy.

#### 712.02 SYSTEM LEVEL ACTIVITIES

- A. The Vice Chancellor for Information Technology shall maintain a security plan and guidelines for inter-institutional computer activities.
- B. The Vice Chancellor for Information Technology shall maintain a computer security implementation handbook which the individual units of the University System of Georgia may choose to use in their individualized implementation schemes.

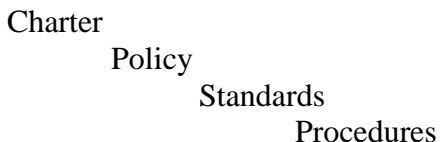
#### 712.03 INSTITUTIONAL RESPONSIBILITIES

- A. The president of each institution shall be responsible for ensuring that appropriate and auditable security controls are in place on his/her campus.

- B. Each institution shall develop, implement and maintain a computer security plan which follows guidelines provided by the Office of Information Technology. Institutions should submit the plan to the Office of Information Technology for review and approval.
- C. The Board recognizes that user education is a vital part of security. Therefore, each institution shall include in its security plan methods for ensuring that information regarding the applicable laws, regulations, guidelines and policies is distributed and readily available to computer users.
- D. Clear and documented procedures for reporting and handling security violations shall be distributed on each campus. The method of providing this information shall be included in the formal plan.
- E. The Regents' Central Office, Skidaway Institute, and any other institutions or institutes added to the University System of Georgia shall develop computer security plans using the same guidelines provided to the institutions (BR Minutes, 1991-92, pp. 391-392).

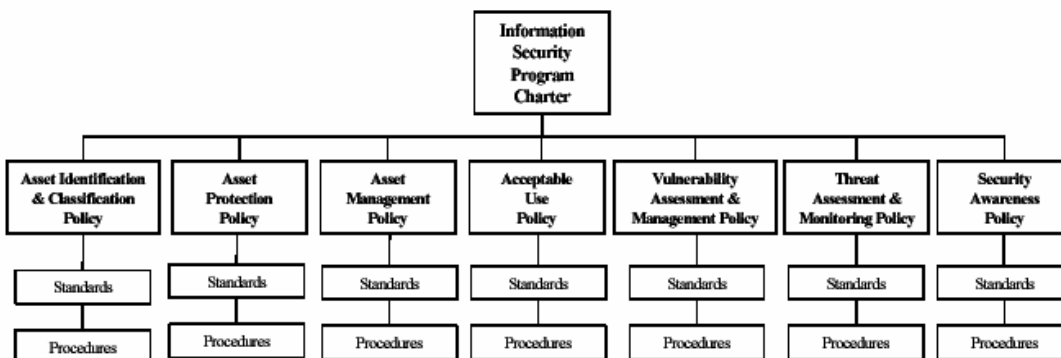
**Policy Structure and Nomenclature**

All IT policies should be built around a defined structure. This structure is hierarchical; ranging from a very high level statement of purpose cascading down to very specific procedures or “How-To” documents. Although in the security field there is no complete consensus on terms, one of the more commonly accepted hierarchical structures is:



It is recommended that the USG follow a similar structure and terminology.

A good example of how this structure works is shown in the following example taken from the Meta Group.



The *Definitions* of Charter, Policy, Standards and Procedures are well stated in a Meta Group Paper as

### **“Information Security Program Charter**

The Information Security Program Charter serves as the capstone document for the Information Security Program and empowers the Information Security Program to manage Information Security-related business risks. The charter summarizes an organization’s attitude and philosophy regarding security. It also states the Information Security Program’s mission to identify, assess, and appropriately mitigate vulnerabilities and threats that can adversely impact the information assets of the organization. In addition, the charter addresses several key program management issues, including scope of coverage, executive ownership, management responsibility, accountability, enforcement, and communication.

The Chief Executive Officer (Board of Regents or Institution President) should approve the Charter to provide justification and executive approval of Information Security program activities. Without this approval, Information Security-related initiatives and activities may be challenged and require individual justification and approval.

### **Policies**

A policy defines an organization’s high-level Information Security philosophy in a topical area. Policies are brief technology and solution independent documents. However, policies provide the necessary authority to establish and implement technology and solution-specific standards. In general, policies remain relevant and applicable for a substantial period of time, and only require revisions when there is a fundamental change to an organization’s business or operational objectives and environment. “ ©Meta 2002

### **Standards**

A security or IT standard is written to cover a specific product, area or process. It implements the broader Policy in a unique area.

### **Procedure**

A procedure is a “How To” document. It is very specific and details commands to be used, forms to be completed, and actions to be taken.

There are many methods of thought as to how to break down the very broad IT Charter into specific policy areas. Since a policy should cover broad areas at a high level, there should only be a need for a limited number of policy areas. However there needs to be enough to allow for good categorization.

The International Standards Organization has done work on defining Security Standards. They have developed the ISO 17799 standard makes use of ten categories. They are:

**1. Security Policy**

Provide management direction and support for information security.

**2. Business Continuity Planning**

Prevent interruptions to business activities and critical business processes caused by major failures or disasters.

**3. System Access Control**

1) Control access to information 2) prevent unauthorized access to information systems 3) ensure the protection of networked services 4) prevent unauthorized computer access 5) detect unauthorized activities. 6) ensure information security when using mobile computing and networking facilities

**4. System Development and Maintenance**

1) Ensure security is built into operational systems; 2) prevent loss, modification or misuse of user data in application systems; 3) protect the confidentiality, authenticity and integrity of information; 4) ensure IT projects and support activities are conducted in a secure manner; 5) maintain the security of application system software and data.

**5. Physical and Environmental Security**

Prevent unauthorized access, damage and interference to business premises and information; prevent loss, damage or compromise of assets and interruption to business activities; prevent compromise or theft of information and information processing facilities.

**6. Compliance**

1) Avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements 2) ensure compliance of systems with organizational security policies and standards 3) maximize the effectiveness of and minimize interference to/from the system audit process.

**7. Personnel Security**

Reduce risks of human error, theft, fraud or misuse of facilities; ensure that users are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work; minimize the damage from security incidents and malfunctions and learn from such incidents.

**8. Security Organization**

1) Manage information security within the Company; 2) maintain the security of organizational information processing facilities and information assets accessed

by third parties. 3) Maintain the security of information when the responsibility for information processing has been outsourced to another organization.

#### **9. Computer & Operations Management**

1) Ensure the correct and secure operation of information processing facilities; 2) minimize the risk of systems failures; 3) protect the integrity of software and information; 4) maintain the integrity and availability of information processing and communication; 5) ensure the safeguarding of information in networks and the protection of the supporting infrastructure; 6) prevent damage to assets and interruptions to business activities; 7) prevent loss, modification or misuse of information exchanged between organizations.

#### **10. Asset Classification and Control**

Maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection.

## Representative Policies and standards

Within each Policy area a number of Standards and then procedures need to be developed. The following table presents some examples of these policies and standards.

<b>Policy</b>	<b>Description</b>
Acceptable Encryption Policy -	Defines requirements for encryption algorithms used within the organization.
Acceptable Use Policy -	Defines acceptable use of equipment and computing services, and the appropriate employee security measures to protect the organization's corporate resources and proprietary information.
Analog/ISDN Line Policy -	Defines standards for use of analog/ISDN lines for Fax sending and receiving, and for connection to computers.
Anti-Virus Process –	Defines guidelines for effectively reducing the threat of computer viruses on the organization's network.
Application Service Provider Policy –	Defines minimum security criteria that an ASP must execute in order to be considered for use on a project by the organization.
Application Service Provider Standards -	Outlines the minimum security standards for the ASP. This policy is referenced in the ASP Policy above.
Acquisition Assessment Policy –	Defines responsibilities regarding corporate acquisitions, and defines the minimum requirements of an acquisition assessment to be completed by the information security group.
Audit Policy -	Defines the requirements and provides the authority for the information security team to conduct audits and risk assessments to ensure integrity of information/resources, to investigate incidents, to ensure conformance to security policies, or to monitor user/system activity where appropriate.
Automatically Forwarded Email Policy –	Documents the requirement that no email will be automatically forwarded to an external destination without prior approval from the appropriate manager or director.
Database Credentials Coding Policy –	Defines requirements for securely storing and retrieving database usernames and passwords.
Dial-in Access Policy -	Defines appropriate dial-in access and its use by authorized personnel.
DMZ Lab Security Policy –	Defines standards for all networks and equipment

	deployed in labs located in the "Demilitarized Zone" or external network segments.
Extranet Policy –	Defines the requirement that third party organizations requiring access to the organization's networks must sign a third-party connection agreement.
Information Sensitivity Policy –	Defines the requirements for classifying and securing the organization's information in a manner appropriate to its sensitivity level.
Internal Lab Security Policy –	Defines requirements for internal labs to ensure that confidential information and technologies are not compromised, and that production services and interests of the organization are protected from lab activities.
Internet DMZ Equipment Policy –	Defines the standards to be met by all equipment owned and/or operated by the organization that is located outside the organization's Internet firewalls (the demilitarized zone or DMZ)).
Internet DMZ Equipment Policy –	Defines the standards to be met by all equipment owned and/or operated by the organization that is located outside the organization's Internet firewalls (the demilitarized zone or DMZ).
Lab Anti-Virus Policy –	Defines requirements, which must be met by all computers connected to the organization's lab networks to ensure effective virus detection and prevention.
Password Protection Policy –	Defines standards for creating, protecting, and changing strong passwords.
Remote Access Policy –	Defines standards for connecting to the organization's network from any host or network external to the organization.
Risk Assessment Policy –	Defines the requirements and provides the authority for the information security team to identify, assess, and remediate risks to the organization's information infrastructure associated with conducting business.
Router Security Policy -	Defines standards for minimal security configuration for routers and switches inside a production network, or used in a production capacity.
Server Security Policy –	Defines standards for minimal security configuration for servers inside the organization's production network, or used in a production capacity.
Third Party Network Connection Agreement –	Defines the standards and requirements, including legal requirements, needed in order to

	interconnect a third party organization's network to the production network. Both parties must sign this agreement.
VPN Security Policy –	Defines the requirements for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the organization's network.
Wireless Communication Policy –	Defines standards for wireless systems used to connect to the organization's networks.

## Resources

Many resources are available to help in Policy Development. Some that might be helpful are:

### Web sites:

Georgia Tech Information Security Site. <http://www.security.gatech.edu/policy/usage/>

Georgia Technology Agency security policies:

[http://www.gagta.com/download/Enterprise\\_Security\\_Policies\\_FINAL091002.doc](http://www.gagta.com/download/Enterprise_Security_Policies_FINAL091002.doc)

SANS Institute Reading Room. <http://rr.sans.org/policy/index.php>

Fraser (Editor), Various (Authors), Various(Reviewers), "RFC 2196: Site Security Handbook", Ohio State University.

<http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2196.html>

The Network Security Library, Various Information Security Papers.

<http://secinf.net/ipolicye.html>

### Bibliography

Wood, Charles Cresson. Information Security Policies Made Easy. Version 8. Baseline Software; ISBN: 1881585077; (May 1, 2001) 740 pages. Contains CD Rom with sample policies. Although this book is pricey at \$559, the CD ROM provides excellent sample policies that can greatly reduce the effort needed to develop a full suite of policies.

Peltier, Thomas R. Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management CRC Press; ISBN: 0849311373; 1st edition (December 20, 2001) 312 pages. List \$69.95.