

# Information Technology (IT) Security Policy

**Issue Date: June 1, 2004**

**Effective Date: June 1, 2004**

**Number: HHSS-2004-002**

## 1.0 Purpose

This policy defines the safeguards deployed to protect HHSS Information Technology (IT) Resources.

## 2.0 Scope

This policy applies to employees, contractors, consultants, temporary employees, volunteers, and other workers employed by HHSS hereafter referred to as staff. This policy applies to all HHSS and State IT resources owned, leased, or supported by HHSS or any outside entity that has signed *Third Party Agreement* with HHSS.

HHSS IT resources referred to in this document include software applications containing protected HHSS data, servers, workstations, networks, and any process or procedure by which these systems are used, administered and/or maintained.

Safeguards defined in this document include the following categories:

- Audits for appropriate use of IT resources.
- Risk assessments of vulnerabilities for appropriate HHSS IT resources.
- Access controls to network and software application systems.
- Electronic and physical safeguards.

## 3.0 Policy

This Policy requires appropriate security safeguards be implemented and monitored to ensure the security, privacy, and confidentiality of the IT resources and tools used to provide HHSS services. Information Systems & Technology (IS&T) a division of Finance and Support is charged with the responsibility for implementing and maintaining reasonable and appropriate security safeguards that meet state and federal statutes as they apply to HHSS and protected HHSS IT resources.

**3.1** Staff granted access to HHSS IT resources must abide by all safeguards listed in this policy and follow the guidelines defined in standards and procedures associated with this policy. Staff will cooperate fully with IS&T in carrying out the safeguards.

**3.2** It is HHSS Policy that to insure appropriate access to and use of IT

resources is maintained, scheduled and random IT audits will be made on IT resources storing or accessing HHSS information. Such audits will be a joint venture between IS&T and the HHSS Department, Division, or Program area being audited.

**3.3** It is HHSS Policy that scheduled and random risk assessments will be conducted on HHSS IT resources maintaining or accessing HSSS information. Such risk assessments will evaluate the potential security risk a defined IT resource's vulnerabilities may have and their potential impact it may have on other HHSS IT resources. The risk assessments will be a joint venture between IS&T and the HHSS Department, Division, or Program area accountable for the IT resource included in a risk assessment.

**3.4** Development and implementation of remediation programs identified as a result of an IT audit or risk assessment is the joint responsibility of IS&T and the HHSS entity responsible for the IT resource being assessed.

**3.5** It is HHSS Policy that appropriate access control safeguards be implemented to protect IT resources from unauthorized access. Access controls include unique identification and authentication of users before access is granted to protected IT resources. Any staff authorized to access a protected HHSS IT resource must be assigned a unique identification (ID). Staff assigned to a unique ID are responsible for protecting access granted using this ID and for all activity performed using their assigned unique ID.

**3.6** It is HHSS Policy that appropriate electronic and physical safeguards must be implemented for any HHSS IT resource containing or accessing critical HHSS information. Electronic and physical safeguards must be appropriate to meet a defined level of risk and updated as required by state and federal statutes and changes in technology.

#### **4.0 Policy Standards**

Associated Standards published subsequent to this policy provide specific guidelines for compliance to the policy. Standards reflect current guidelines and may be updated as necessary to meet changes in state and federal rules and regulations and changes in technology implemented in HHSS.

[Information Technology \(IT\) Security Audit Standard](#)

[Information Technology \(IT\) Risk Assessment Standard](#)

[Information Technology \(IT\) Access Control Standard](#)

[Information Technology \(IT\) Incident Reporting Standard](#)

#### **5.0 Enforcement**

Should a violation of this Acceptable Use Policy occur, the individual who committed the violation shall be personally responsible for their own actions and any reasonably foreseeable consequences of those actions. Any employee found to have violated this policy may be disciplined in accordance with the applicable workplace policies and labor contracts. Such discipline may include termination of employment.

## **6.0 Revision History**

*HR Legal – March 12, 2004*

*Policy Title: Information Technology (IT) Security Policy*

*Policy Approved: April 13, 2004*

*Policy Effective: June 1, 2004*

*Policy Owner: Information Systems & Technology*

*Agency: Finance and Support*

*Adopted by the Policy Cabinet: April 13, 2004*