BLUEPRINT INTERGOVERNMENTAL AGENCY **Administrative Procedures Manual**	DATE September 7, 2006 NO. **109**
TITLE **SECURITY AND USE OF INFORMATION TECHNOLOGY RESOURCES, INCLUDING E-MAIL, INTERNET, AND ANTI-VIRUS SOFTWARE**	ORG. AGENCY Blueprint Intergovernmental Agency APPROVED

109.01 STATEMENT OF POLICY

It is the policy of Blueprint Intergovernmental Agency (the "Agency") that a standard method for information systems security be established.

109.02 AUTHORITY

Director of PLACE.

109.03 OBJECTIVE

The purpose of this policy, and its provisions, is to serve as a guide to all Blueprint and OEV staff.

109.04 SCOPE AND APPLICABILITY

These procedures apply to all Blueprint and OEV staff members who may be assigned, or have access to, an Agency computer or a personal computer with remote access.

109.05 SECURITY PROCEDURES

Security procedures are categorized in the major headings below. The entire procedure is described under the each major heading.

1. GENERAL REQUIREMENTS

It is the policy of the Agency to treat information and information technology resources as strategic assets. As such, these assets must be protected from misuse, abuse and loss through the management of a comprehensive information technology resources security program.

1.1 The Director of PLACE or his/her Designee serves as the Agency's Information Security Manager, and is responsible for administering the Agency's data and information technology resources security program. The Director of PLACE will designate an appropriate staff person within the Agency's office to assist in administering the information technology resources security program. This person will be responsible and accountable for ensuring access controls are properly maintained for computer network resources. All persons within the Agency that develop computer systems security for their specific data shall coordinate their security efforts with the assigned staff person.

1.2 The Agency's information technology resources security program is defined within the following areas:

(1) Personnel Requirements for Security
(2) Confidentiality of Information & Data
(3) Control of Computers and Information Resources
    a. Electronic Mail
    b. Internet
    c. Hardware and Software
(4) Physical Security and Access to Data Processing Facilities
(5) Logical and Data Access Controls
(6) Network Security
(7) Protection Against Loss

1.3 This policy shall apply to all information systems and persons that access, process, or have custody of data at all sites of the Agency. This includes all owned, leased, and contracted services involving mainframe, microcomputer, distributed processing, and networking environments.

1.4 Any request for a change or exception to this policy may be submitted to the Director of PLACE or his/her Designee for a decision

2. PERSONNEL REQUIREMENTS FOR SECURITY

2.1 Each individual with authenticated access to Agency information technology resources is required to adhere to this policy and all information security standards and procedures.

2.2 Each individual accessing Agency information technology resources is expected to use good judgment and common sense in the workplace to avoid abuse and inappropriate use of resources. It is inappropriate to use any resource which will: interfere with the timely performance of an individual's normal work duties; cast disrespect or adverse reflection upon the Agency; reduce public confidence; support a personal business; support political or religious activities; or detract from the Agency's routine functions. Furthermore, it is inappropriate for employees to access, send, store, create, or display sensitive materials including, but not limited to, gambling, any illegal activity, sexually explicit materials, or materials that include profane, obscene, or inappropriate language, or discriminatory racial or ethnic content. Such activities will be considered misuse or abuse of information technology resources.

2.3 Each individual with authorized access to Agency information technology resources shall be held responsible for systems security to the degree that his or her job requires the use of information and associated systems. All users are responsible for using information technology resources only for the purpose intended, to comply with all controls

established by information technology resource owners and custodians, for protecting sensitive information against unauthorized disclosure, and for protecting the Agency from unauthorized access to information resources including physical connections to the Agency network.

2.4 Each individual who uses licensed or copyrighted software must adhere to the terms and conditions of the license or copyright. In addition, all copyrights and rights of licensure must be adhered to in the use of material on the Internet.

2.5 Each individual that has been granted privileged or specialized security authorizations will be considered to be in a position with trusted security requirements. This includes, but is not limited to, individuals that grant security authorizations, administer networks and servers, use voice and telecommunications diagnostic equipment, use remote control software, migrate software and code from test to production environments, or perform other security related activities deemed sensitive or critical by their manager or supervisor.

2.6 Compliance with information technology resource security requirements is mandatory and misuse or abuse can result in disciplinary actions up to and including dismissal, civil penalties, or criminal penalties. Whoever willfully, knowingly, and without authorization accesses or causes to be accessed any computer, computer system, or computer network commits an offense against computer users as defined in ***Chapter 815, Florida Statutes, Computer Related Crimes***.

2.7 All users are responsible to immediately report any violations of this policy to the Director of PLACE or his/her Designee.

3. CONFIDENTIALITY OF INFORMATION AND DATA

3.1 Information systems access shall be limited to individuals having an authorized need to use the information. Data file and program access will be limited to those individuals authorized to view, process, or maintain particular systems. Confidential data (data that has been legally determined to be exempt from public records requests as defined by ***Chapter 119, Florida Statutes, Public Records***, and sensitive data (data that is subject to a public records request but otherwise should be accessible only to authorized personnel on the basis of a strict "need to know" for the performance of their duties) must be made readily identifiable by the owner and treated as confidential or sensitive in its entirety. A sufficiently complete history of transactions will be maintained for each session involving access to critical and sensitive information, as determined by risk analysis and technical feasibility, to permit an audit of the system.

3.2 While the Agency intends to provide a reasonable level of confidentiality, users should have no expectation of privacy since the data they create or receive on the Agency

network system is the property of the Agency and is therefore subject to the requirements of ***Chapter 119, Florida Statutes, Public Records.***

4. CONTROL OF COMPUTERS AND INFORMATION RESOURCES

All information technology resources owned or leased by the Agency are to be used to carry out the mission of the Agency and to promote efficiency and improved communications with our internal and external customers. It is intended that information technology resources be used for business purposes.

4.1 ELECTRONIC MAIL (E-MAIL)

4.1.1 Employees will be granted use of electronic mail (e-mail) to carry out the mission of the Agency and to promote efficiency and improved communications with our internal and external customers. It is intended that e-mail be used for business purposes. E-mail is only authorized through the Agency's official e-mail and Internet applications.

4.1.2 Although it is intended that e-mail be used for business purposes, good judgment and a common sense approach must be used. For example, acceptable uses of e-mail can be compared to those involving use of a telephone where, at times, personal messages are conveyed. However, such messages must be brief and infrequent and not constitute inappropriate use as described in ***Section 2*** of this policy.

4.1.3 The Agency will conduct random reviews of e-mail, through direct access or the use of archival data, to detect abuse or misuse of these resources, with or without notice to the employee. Deletion from an employee's file does not constitute deletion from the archived files. E-mail is not private and may be subject to the requirements of ***Chapter 119, Florida Statutes, Public Records***.

4.1.4 Misuse or abuse of e-mail may result in disciplinary action defined in ***Section 2*** of this policy.

4.2 INTERNET

4.2.1 Employees will be granted use of the Internet to carry out the mission of the Agency and to promote efficiency and improved communications with our internal and external customers. It is intended that the Internet be used for business purposes.

4.2.2 Although it is intended that the Internet be used for business purposes, access to other acceptable sites is permitted within reason. Examples of acceptable Internet sites are: health matters, weather, news, business topics, community activities, and career advancement. Under certain circumstances, such as emergency weather conditions, access to sites such as weather and news services may be appropriate within approved working hours.

4.2.3 The Agency Office will randomly review records of all Internet usage for use in detecting abuse or misuse of this resource with or without notice to the employee.

4.2.4 Misuse or abuse of the Internet may result in access being revoked, which could result in an employee being unable to perform the job functions of his or her class specification and/or the disciplinary action defined in ***Section 2*** of this policy.

4.3 HARDWARE AND SOFTWARE

4.3.1 All computer hardware and software used by Agency personnel in the performance of their duties for the Agency will be Agency owned or leased. The only two exceptions will be: 1) authenticated remote access and 2) special circumstances. Both shall be approved by the Director of PLACE or his/her Designee.

4.3.2 If an exception is approved, it is the responsibility of the equipment owner to implement appropriate security controls to safeguard their equipment. The Agency will not provide support to non-Agency owned or leased hardware or software and will not be liable for any damage resulting from connectivity to Agency information technology resources.

4.3.3 Only authorized personnel will use software that allows one to observe or control a remote computer. Remote control will be used for the sole purposes of testing, systems maintenance, troubleshooting, and user support. This software must provide an “acceptance” or “notification” mechanism to a remote user, informing them that their computer is under remote control.

4.3.4 A user may not install personal hardware or software on Agency equipment unless it is specifically approved by the Director of PLACE or his/her Designee. Exporting software, technical information, encryption software or technology in violation of international or regional export control laws is illegal.

4.3.5 Under no circumstances will game or entertainment software be used on Agency owned or leased machines. Games are not to be used for training.

4.3.6 When it is beneficial to the Agency and approved in advance by the employee's supervisor or higher management, Agency owned or leased personal computers may be used for educational and training purposes for the following programs or related courses: Any course that meets a work-related need as determined by the supervisor, including courses taught by or for the Agency. This does not include tuition waiver courses taken by employees at a state university on a space available basis. This policy shall not be construed to prohibit the authorized evaluation of hardware, software, or new technologies.

5. PHYSICAL SECURITY AND ACCESS TO DATA PROCESSING FACILITIES

5.1 Information shall be created and maintained in a secure environment. The cost of security shall be commensurate with the value of the information, considering value to both the Agency and to a potential intruder. Measures with respect to the creation and maintenance of information will be taken to ensure against the unauthorized modification, destruction, or disclosure of information by any person at any location, whether accidental or intentional. Safeguards will be established to ensure the integrity and accuracy of Agency information that supports critical functions of the Agency, and for which processing capabilities must be provided in the case of a disaster.

6. LOGICAL AND DATA ACCESS CONTROLS

6.1 Access to information technology resources is authorized for a specific individual and must be used exclusively by that individual. Access passwords must not be shared or entered by any automatic means, such as with macros. It is the user's responsibility to protect all of his or her passwords from being disclosed and to refuse identification of any other user's password.

7. NETWORK SECURITY

7.1 Computer hardware may never establish simultaneous network connections between an Agency network and any other non-Agency network unless it is specifically approved by the Director of PLACE or his/her Designee. Unauthenticated access is prohibited.

7.2 Any request to connect an external network to the Agency's data communications network must be documented and approved by the Director of PLACE or his/her Designee. Prior to establishing such connections, appropriate security controls, such as firewalls, must be implemented to protect the Agency's network from unauthorized access.

7.3 Only individuals authorized by the Director of PLACE or his/her Designee can use voice and data telecommunications diagnostic hardware and software such as communications line monitors. Use is restricted to testing, monitoring, and troubleshooting, unless specifically authorized in writing for other business related activities by the Director of PLACE or his/her Designee.

7.4 Only individuals authorized by the Director of PLACE or his/her Designee may access the Agency's network through remote access connection VPN. Individuals who require remote VPN access must utilize Agency provided hardware (PCs).

8. PROTECTION AGAINST LOSS

8.1 All Agency owned or leased microcomputers and servers must have an anti-virus

software program installed and operating at all times. The Agency provides software for this purpose and distributes updates. Appropriate configurations include real-time protection to support ongoing or background scans whenever a "create, open, move, copy or run" command is performed. This configuration should not be altered by any user. In all instances, electronic data, software, or documents must be scanned for viruses before being used on an Agency computer. It is the responsibility of vendors, consultants, or contractors to ensure that electronic media provided to the Agency is not infected. Infected electronic media will be returned and will not be accepted by the Agency.

8.2 Data and software essential to the continued operation of critical Agency functions shall be backed up. The security controls over the backup resources shall be as stringent as the protection required of the primary resources.

109.06

EFFECTIVE DATE

This policy will become effective September 7, 2006.

Revised: February 21, 2017