NJ OFFICE OF INFORMATION TECHNOLOGY
Chris Christie, Governor
Dave Weinstein, Chief Technology Officer

P.O. Box 212
300 Riverview Plaza
Trenton, NJ 08625-0212

www.tech.nj.gov

STATE OF NEW JERSEY TECHNOLOGY CIRCULAR 183 - Software License Management and Distribution Policy	**POLICY NO:** 14-12-NJOIT	
	SUPERSEDES: NEW	**EFFECTIVE DATE:** 04/03/2014
	VERSION: 1.0	**LAST REVIEWED:** 04/03/2014

ATTN: Directors of Administration and Agency IT Leaders

1 PURPOSE

Information technology software is provided by State government entities to employees and other authorized individuals to assist them with their assigned work responsibilities and duties. Acceptable use is dictated by license agreements, laws and regulations, and this policy's purpose is to prevent prohibited usage by Executive Branch employees and other users of State systems. Agencies may supplement this policy as needed, as long as such supplement is consistent with the content and intent of this policy.

2 AUTHORITY

This policy is established under the authority of the State of New Jersey. N.J.S.A. 52:18a-230 b. This policy defines New Jersey Office of Information Technology's (NJOIT) role with regard to technology within the Executive Branch community of State Government.

The New Jersey Office of Information Technology (NJOIT) reserves the right to change or amend this circular.

3 SCOPE

This policy applies to all State Departments, Agencies, "in but not of" entities, their employees, contractors, consultants, temporary workers, and others who develop and administer information systems and resources for systems maintained by the Executive Branch.

By accessing the State's network or software applications, a user agrees to adhere to the State's policies, including agency specific policies, regarding their use.

4 POLICY

4.1 Users are prohibited from the following:

4.1.1 Infringing intellectual property and copyright laws. Users must abide by the State's Division of Purchase and Property's terms and conditions of the applicable copyright law. Violations of copyright law generally include but are not limited to illegally copying, distributing, downloading, and/or uploading information from the Internet (or any electronic source) without the permission of the copyright owner. Examples of commonly copyrighted items are audio materials, movies, videos, software and images.

4.1.2 Downloading, attaching, changing, distributing, copying or installing any software illegally or without proper authorization.

4.1.3 Downloading, attaching, changing, distributing, duplicating or installing any inappropriate files, including streaming content, for non-business functions (e.g. downloading MP3 files and/or broadcast audio or video files).

4.1.4 Intentionally introducing malware onto a State-provided computer, or withholding information necessary for effective malware control procedures.

4.1.5 Using State-provided computer hardware and software to play or download games, audio, or videos that are not in support of State business functions.

4.1.6 Copying, installing, altering, deleting, or destroying any data or computer software unless specifically and legally authorized.

4.1.7 Downloading and installing unauthorized and/or undocumented freeware or shareware.

4.1.8 Storing software and licenses on a public storage service. Further, no software or licenses can be stored on a public device or drive from which unauthorized duplication or installation can occur.

4.1.9 Installing State software on home or user-owned computers or personal devices without authorization.

4.2 Only authorized software shall be installed or used on State-owned or leased hardware. All Agencies shall implement the following controls:

4.2.1 Ban use of unlicensed software copies (software used in violation of the software license), or software not authorized by the agency.

4.2.2 Publish a software copyright compliance procedure which defines the legitimate use of software and information products. Legitimate use consists of obtaining and maintaining a copy of the license agreement and authorization to install the software.

4.2.3 Maintain awareness of the software copyright and acquisition procedures and give notice of the intent to take disciplinary action against staff who breach those procedures.

4.2.4 Keep current with patches or upgrades of all software that the State supports. Patches and upgrades should be licensed or approved by the licensor. To protect security and minimize incompatibility issues, agencies must use current versions of software that have all required patches and upgrades in place. The State should not use products that are no longer supported by the licensor. Any exceptions must be approved as specified in Section VI of this IT circular.

4.2.5 Establish and maintain an asset and software inventory to register, track and control all authorized software media, licenses or end-user license agreements, certificates of authenticity, documentation and related items.

4.2.6 Establish a software management and distribution system to assist in tracking, distributing and managing agency's authorized software. The system should provide proactive and automated processes to build and deploy computer systems, and verify software license and security compliance.

4.2.7 Document and ensure that the maximum number of users permitted by a license is not exceeded.

4.2.8 Maintain proof and evidence of ownership of licenses, master disks, manuals, etc.

4.2.9 Conduct documented annual software compliance reviews and physical inventories of libraries and computer systems to determine whether the agency and its users are complying with applicable software license agreements and State/Agency standards and procedures.

4.2.10 Dispose of software in accordance with the software publisher's or manufacturer's license or copyright agreements, agency policy and state procedure.

5 RESPONSIBILITIES

5.1 Employees

5.1.1 Employees shall follow this policy and all agency software usage policies and procedures. Users should report any misuse or policy violations to their supervisors or Agency IT Directors.

5.2 Executive Branch Departments and Agencies

Agencies shall develop internal guidelines, procedures, and controls for monitoring compliance in accordance with this policy.

Agencies shall furnish their current employees with copies of this notice, and shall furnish all new employees with copies of this policy concurrent with authorizing them to use agency computers.

Agencies shall take appropriate administrative actions for violations of this policy or any standards or guidelines referenced.

Agencies shall promote the awareness of the acceptable use of State software applications by training employees in the use of procedures to access these applications.

Agencies shall identify who will be the installation authority responsible for software license management and distribution. Among other duties, this designee must ensure that procedures are in place for the proper licensing, including documentation, of each piece of Enterprise software (software available for use by an entire agency or unit). These procedures must include a clear explanation of how the licensing agreement applies to the user, including terms and conditions for use.

To ensure that only authorized computer software is acquired for and used on agency's computers, each department/agency IT Director will ensure compliance with U.S. copyright laws and with the provisions of this policy.

6 EXCEPTIONS AND NON-COMPLIANCE

Departments and Agencies shall comply with this policy within 90 days of its effective date.

Requests for exceptions for non-compliance with this policy shall be processed in accordance with Statewide IT Circular *08-02-NJOIT*, 111 – Information Security Managing Exceptions.

7 REFERENCES

Computer Fraud and Abuse Act of 1986

Signature on File | *4/3/2014*

E. STEVEN EMANUEL | **DATE**

Chief Technology Officer-NJ Office of Information Technology

State Chief Information Officer