I. PROCEDURE OVERVIEW

The purpose of this procedure is to establish management direction, and requirements for granting privileged access to NYSDOT computer systems, applications and information. To preserve the integrity, confidentiality and availability of New York State Department of Transportation’s (hereafter NYSDOT) information assets, the Department will use logical and physical access control mechanisms commensurate with the value, sensitivity, consequences of loss or compromise, legal requirements and ease of recovery of those assets.

This procedure applies to all computer systems, communications networks, applications and information owned or operated by NYSDOT. This procedure applies to all employees, vendors, contractors, subcontractors, consultants, sub-consultants, volunteers, individuals doing research, student interns, temporaries, and other entities including those users affiliated with third parties and other organizations that access NYSDOT computer networks, systems, applications or information. Throughout this procedure, the words “Information User” and “User” will be used to collectively refer to all such individuals. This specifically includes maintenance and service personnel.

II. PROCEDURE DEFINITIONS AND ROLES OF PARTICIPANTS

Definitions

In order to provide clarity and consistency, terms used in this procedure and other security policies are defined in the Security Policy Project Glossary.

Privileged access enables an individual to take actions which may affect computing systems, network communication, or the accounts, files, data, or processes of other users. Privileged access is typically granted to system administrators, security administrators, database administrators, staff performing computing account administration, or other such employees whose job duties require special privileges over a computing system or network.

An attribute is a characteristic associated with an individual or organization. Access to systems, applications and information is granted based on those relevant attributes. In a security system, an attribute is a field associated with an individual’s profile in a security system. Each Information User has a security profile which is a record in a computer file.
The record contains information about the user and attributes that refer to the user’s access permissions to all applications. Each application will have an attribute associated with it. The security software or application software will allow access to a specific application after the user has authenticated, by use of the unique user-ID and password combination and if the user has the appropriate attribute or combination of attributes that indicate access has been authorized.

A **category of staff** is a group of Users defined by a common set of attributes.

The **principle of least privilege** requires that a User be given no more privilege than necessary to perform an authorized job or task. Ensuring least privilege requires identifying what the user's job is, determining the minimum set of privileges required to perform that job, and restricting the user to those privileges and nothing more. Privileges should be granted only for the timeframe required for the job. The principle of least privilege will be employed requiring that access control permissions for all systems must be set to a default which blocks access by unauthorized users and every information system privilege which has not been specifically allowed is forbidden.

The **principle of security in depth** refers to the implementation of a security defense in multiple layers of different types to provide substantially better protection. The **principle of security in depth** will be employed requiring access control at each layer of the system including network, hardware devices, system software, application and data.

**Responsibilities**

**Information Owners** are responsible for determining who should have access to protected resources, what those privileges will be (read, update, etc.) and for monitoring appropriate use. These access privileges will be granted in accordance with the user’s job responsibilities. For granting privileged access, the designated Owners shall be the Director of the Information Services Bureau and the Information Security Officer. In addition, where user data is involved, the Information Owner of that data must also approve the access.

**Individual Accountability** is required when accessing all NYSDOT electronic resources. Access to computer systems and networks must be provided through the use of individually assigned unique computer identifiers, known as user-IDs. Individuals who use NYSDOT computer resources must only access resources to which he or she is authorized. Associated with each user-ID is an authentication token, such as a password, which must be used to authenticate the person accessing the data, system or network. Passwords must be treated as confidential information, and must not be disclosed. All individuals are responsible for all activities performed under their user-ID. For the user’s protection, and for the protection of NYSDOT resources, user-IDs must not be shared.

**III. PROCEDURAL GUIDELINES**

The issuance and use of privileged accounts will be restricted and controlled. Inappropriate use of system privileges is often found to be a major contributing factor to the failure of
systems that have been breached. Use of privileged accounts will be monitored and any suspected misuse of these accounts will be promptly investigated and appropriate action taken.

Individuals with privileged access must respect the rights of the system users and the integrity of the systems and related physical resources. These individuals also have an obligation to inform themselves regarding any procedures, business practices, and operational guidelines pertaining to the activities of NYSDOT systems.

Individuals with privileged access must comply with applicable policies, laws, regulations, procedures, and standards while pursuing appropriate actions required, providing secure and reliable computing services.

Where the technology permits, individual user-IDs must be assigned to each person with privileged access.

**Access Basic Principles**

Access to systems and information will be granted only when a legitimate business need has been demonstrated, access has been approved in advance by the Information Owner and all applicable policies, procedures and requirements have been complied with. Such approvals may be granted to a category of staff based on appropriate attributes. Owners may request a higher level of protection and more limited privileges where they deem it appropriate.

The principle of least privilege will be employed requiring that access control permissions for all systems must be set to a default which blocks access by unauthorized users and every information system privilege which has not been specifically allowed is forbidden.

The principle of security in depth will be employed requiring access control at each layer of the system including network, hardware devices, system software, application and data.

Information about security measures for computer systems, networks, applications and information is confidential and should not be released to anyone who is not an authorized user of the involved systems unless the permission of the Information Security Officer has first been obtained.

The security of information and systems applies to all locations with access to NYSDOT systems.

**Separation of Duties**

Whenever a computer-based process involves sensitive or critical information, the system must include controls involving a separation of duties or other compensating control measures. There must be an appropriate separation of duties for functions including system administration, network administration, database administration, application development, computer operations and control, support services and information security. These control measures must ensure that no one individual has exclusive control over these types of
information assets or functions related to them. Roles and responsibilities must be divided to
the extent practical to assure proper checks and balances. Granting of privileged access must
be done by someone other than the one receiving access.

Privileged Access Requirements
Privileged access may be used only to perform assigned job duties. If methods other than
using privileged access will accomplish an action, those other methods must be used, unless
the burden of time or other resources required clearly justifies using privileged access.

Privileged access may be used to perform standard system-related duties. Examples may
include:

- Installing system software
- Relocating other individuals' files
- Performing repairs required to return a system to normal function, such as fixing files
  or file processes, or killing runaway processes
- Running security checking programs

Privileged access may be used for authorized account management activities to grant,
change, or deny resources, access, or privilege to a User. Under exceptional circumstances,
extraordinary actions may be taken provided that all NYSDOT policies, guidelines and
procedures are followed. Examples may include:

- Disabling an account apparently responsible for serious activities such as: making
  attacks on root (UNIX) or the administrator account (NT), or using a host to send
  harassing or threatening email, or using software to mount attacks on other hosts or
  engaging in activities designed to disrupt the functioning of the host itself;
- Disconnecting a host or subnet from the network when a security compromise is
  suspected and
- Accessing files for law enforcement authorities with a valid subpoena.

In all cases, access to other individuals' electronic information shall be limited to the least
perusal of contents and the least action necessary to resolve a situation.

Individuals with privileged access shall take necessary precautions to protect the
confidentiality of information encountered in the performance of their duties.

If, during the performance of their duties, individuals with privileged access inadvertently see
information possibly indicating inappropriate use, they must notify their supervisor and the
ISO.

Configuration Management
Configuration management is the process of keeping track of changes to the system and
networks and assuring that all changes are properly reviewed and authorized. Configuration
management normally addresses hardware, software, networking, and other changes. The
primary information security goal of configuration management is ensuring that changes to a
system do not unintentionally or unknowingly diminish its security. Therefore all
configuration management must be performed consistent with security policies, procedures and standards. All privileged access must use configuration management procedures and standards for all systems.

**Account Management**
All privileged access control accounts must be documented, tracked and periodically reviewed. This documentation must be treated as highly sensitive and confidential information and be secured in accordance with applicable data classification requirements. It should at a minimum:

- Identify the category of staff who should have access to privileged accounts and/or functions,
- Allocate the highest system privileges only according to specific need, not as a matter of course,
- Allocate privileges to network and/or application software accounts on an 'as needed' basis. The account name should not indicate its associated privilege,
- Provide for unique user-IDs to permit users' actions to be linked to named individuals,
- Identify specific business applications to which access is granted,
- Require a written statement signed by the appropriate Information Owner, the Director of ISB and the ISO, authorizing the access rights and conditions,
- Include formal records documenting periodic reviews of access rights,
- Document account revocations for staff who change jobs within the organization, and for those who leave the organization and
- Document privileges to ensure that a user is allocated the correct range of system privileges for the job in question.

**System Privileges and Administration**
Special system privileges must be restricted to those directly responsible for systems administration and/or systems security. System Administrators must perform configuration changes, operating system changes, and related activities that require “root or administrator” privileges. System Administrators must comply with all user-ID and password requirements and NYSDOT security policies, procedures and standards.

System administrators must have at least two user-IDs. One of these user-IDs must provide privileged access and be logged; the other must be a normal user-ID for the day-to-day work of an ordinary user.

All system-level passwords (e.g., root, enable, NT admin, database, administration, security application administration accounts, etc..) must be changed at least every 30 days.

All privileged user-IDs and passwords must be encrypted during transmission.

Remote administration of Internet-connected computers is not allowed unless one-time passwords are employed over encrypted links.
Employment Practices
All individuals who are provided privileged access rights are subject to background investigations and periodic reviews at the discretion of NYSDOT or as required by applicable statute, regulation or policy.

Non-compliance with these and other information security requirements can result in loss of access to systems and data, disciplinary action up to and including termination and other civil and criminal penalties as may be applicable.

IV. STEPS IN PROCEDURE

Privileged access user-IDs and changes in privileges must be requested and approved by the User's Manager and authorized by the appropriate Information Owner. In the case of privileged access, the Information Owner will be the organization supporting the applications or system requiring privileged access. This would include the Information Services Bureau and Transportation Management Centers. Access can only be granted following current access approval instrument as established by the ISO. The current access approval method can be found on IntraDOT in the Information Security section.

The privileges granted remain in effect until the user's job changes or the user leaves subject to periodic review as described herein. In the event of such a change, the user manager must immediately notify appropriate parties as detailed in the computer account administration process.

V. FORMS IN PROCEDURE

Current form is available on IntraDOT under the security section.

VI. RELATED AUTHIORITATIVE SOURCES

NYS:
New York State Office for Technology Policy 97-1 on Information Security
New York State Information Security Policy –Cyber Policy P03-002

NYSDOT:
NYSDOT General Security Policy 2.18.2.0
Roles and Responsibilities Procedure 2.18.2.5
Data Security Procedure 2.18.2.10
Non-Disclosure Procedure 2.18.2.4
Access Control Procedure 2.18.2.7
Acceptable Use Policy 2.18.2.6
Remote Access Procedure 2.18.2.11
Use and Dissemination Procedure 2.18.2.25