I. PROCEDURE OVERVIEW

The purpose of this procedure is to establish direction and requirements for access to New York State Department of Transportation (hereafter NYSDOT) data, information and systems. To preserve the integrity, confidentiality and availability of NYSDOT’s information assets, NYSDOT 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 data, information and systems owned or operated by NYSDOT at all locations with access to NYSDOT systems. It applies to all vendors, contractors, subcontractors, consultants, sub-consultants, staff augmentation consultants, volunteers, individuals doing research, student interns, temporary employees, and other persons including those Users affiliated with third parties and other organizations that access NYSDOT data, information and systems. Throughout this procedure, the words Information User and User will be used to collectively refer to all such individuals.

II. PROCEDURE DEFINITIONS AND ROLES OF PARTICIPANTS

Access to data, information and systems 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. When a User no longer has a need for system access by reason of job reassignment, retirement, termination of contract, end of project, etc. all system privileges must cease, and access to information must likewise cease.

User privileges must be defined so Users cannot gain access to, or otherwise interfere with, the individual activities of other Users or any data that the Information Owner has not specifically authorized access to for that User.

LEAST PRIVILEGE

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.
SECURITY IN DEPTH

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, applications and data.

SEPARATION OF DUTIES

Whenever a business process involves sensitive or critical information, the system must include controls involving a separation of duties or other compensating control measures. These control measures must ensure that no one individual has exclusive control over these types of information assets or functions related to them. An example of a lack of separation of duties is where a single person has control of issuing checks and maintaining the financial transaction history data.

Whenever practical, no person should be responsible for completing a task involving sensitive or critical information from beginning to end. Likewise, a single person must not be responsible for approving his or her own work. To the extent possible, for every task at least two people must be required to coordinate their information-handling activities.

ACCEPTABLE USE

When the Acceptable Use Procedure, MAP 2.17.2.6, is fully approved and implemented, all Users requiring authorization to use NYSDOT data, information and systems that are connected to NYSDOT internal networks will be required to sign an Acceptable Use Agreement prior to being issued a user-ID. The User’s signature will indicate the involved User understands and agrees to abide by all policies, directions and procedures related to computers, networks, applications and data that NYSDOT issues.

NON-DISCLOSURE OF INFORMATION

All outside parties with access to NYSDOT data, information and systems must refrain from disclosing any information deemed non-Public by NYSDOT. For outside parties employed under a contract, purchase order, or agreement, a standard Information Security Confidentiality Clause will be included in all agreements, contracts, and purchase orders between NYSDOT and the outside party being granted access to NYSDOT data, information and systems. A written Non-Disclosure Agreement will be used for all individuals or entities that are providing services to NYSDOT (requiring access to confidential data) but are not under contract with NYSDOT. Examples of persons providing services to NYSDOT who are not under contract would include student interns, volunteers, instructors, professors, guest speakers, and members of professional organizations. (Refer to NYSDOT Non-Disclosure Procedure 2.18.2.4).

USE AND DISSEMINATION OF INFORMATION

A number of local, state and federal agencies, authorities, consortiums and other NYSDOT business partners routinely share data with NYSDOT. These outside entities will be required to enter into a Use and Dissemination Agreement with NYSDOT when the Use and Dissemination Procedure, MAP 2.18.2.25 is fully approved and implemented. In the
circumstance where a Use and Dissemination Agreement is in place, a Non-Disclosure Agreement will not necessary.

**DISCLOSURE OF SECURITY MEASURES**

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 systems involved unless the permission of the Information Security Officer (ISO) has first been obtained.

**ACCESS CONTROL**

Access control is any mechanism to provide access to data. For computer access, a User must first log in to a system, using an appropriate authentication method. The access control mechanism controls what operations the User may or may not perform by comparing the user-ID to an access control list.

Access control systems include:

- File permissions, such as create, read, edit or delete on a file server
- Program permissions, such as the right to execute a program on an application server
- Data rights, such as the right to retrieve or update information in a database

Access control procedures are the methods and mechanisms used by Information Owners to approve permission for Users to access data, information and systems.

**AUTHENTICATION**

Authentication is the process of identifying an Information User by the User presenting credentials. In a computer system, this is most often accomplished by using the unique user-ID and password combination which is assigned to and known only by the Information User. Other techniques of authentication may be employed with ISO approval.

**SYSTEM**

A system shall be defined as an interconnected set of information resources under the same direct management control that shares common functionality. A system may include hardware, software, information, data, applications or communications infrastructure.

A production system is a system that is used to process information or support on-going business functions. Information systems which have been designated production systems have security requirements defined that are based on the business need.

**INDIVIDUAL ACCOUNTABILITY**

Individual accountability is required when accessing all New York State and NYSDOT electronic resources. Access to computer systems and networks must be provided using individually assigned unique computer identifiers, known as user-IDs. Individuals who use
New York State 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, information or system. Passwords must be treated as confidential information, and must not be disclosed. Each individual is responsible to reasonably protect against unauthorized activities performed under their user-ID.

**INFORMATION OWNERS**

Information Owners are responsible for determining who should have access to protected resources and what those access privileges will be (read, update, etc.). These access privileges will be granted in accordance with the Information User's job responsibilities. Information Owners may delegate administrative responsibility but are ultimately accountable for the information. (Refer to MAP 2.18.2.5 Information Security Roles and Responsibilities Policy).

**USER MANAGERS**

User Managers have a pivotal roll in the security of NYSDOT information. It is the responsibility of User Managers to document and request system access on behalf of Information Users when access is required in the performance of duties. It is the responsibility of the User Manager to request the User's access be revoked in the event of a change in job responsibilities or status of an Information User. (Refer to MAP 2.18.2.5 Information Security Roles and Responsibilities Policy).

**INFORMATION SECURITY LIAISONS**

The Information Security Liaison serves as a primary point of contact between their Program Areas and the ISO on informational and operational security issues. Each Program Area and Region must assign the role of Information Security Liaison. These responsibilities may be fulfilled by the IT Coordinator or IT Manager. The Information Security Liaison shall validate requests for User access to data, information and systems from supervisors or managers and authenticate the requestor. The Information Security Liaison will also provide information security support for their constituents and provide feedback to the ISO regarding problems with policy and security issues. (Refer to MAP 2.18.2.5 Information Security Roles and Responsibilities Policy).

**III. PROCEDURAL GUIDELINES**

**AUTHENTICATION AND IDENTIFICATION**

All computers connected to the NYSDOT network must have an authentication mechanism such as a user-ID and password for access control. Multi-user systems must employ user-IDs and passwords unique to each User, as well as User privilege restriction mechanisms. All workstations whether connected to the network or not, must employ hardware or software controls approved by the ISO and implemented by the system administrator that prevent unauthorized access.
All Users must be positively identified prior to being able to use any data, information or system. Positive identification for internal networks involves both a user-ID and a password, both of which are unique to an individual User.

Users must not use the same user-ID or password that they use for access to NYSDOT systems and information to access non-NYSDOT systems, including any Internet accounts. If NYSDOT participates in the New York State Directory Service (NYSDS), the User’s NYSDOT or NYeNET user-ID and password will be accepted by the other participating organizations.

**Note:** In circumstances where there is a clear business requirement or technologies require shared user-IDs and passwords, approvals may be granted by the affected Information Owners and ISO. An appropriate individual accountability method must be implemented.

The log-in process for network-connected computer systems must simply ask the User to log-in, providing prompts as needed. Specific information about the organization managing the computer, the computer operating system, the network configuration, or other internal matters must not be provided until a User has successfully provided both a valid user-ID and a valid password. If any part of the log-in sequence is incorrect, the User must not be given any information about the source of the problem but simply be informed that the attempt failed.

**Unique User-IDs**

Each user-ID must be unique and forever connected solely with the User to whom it was assigned. After a User is removed, there must not be any re-use of the involved user-ID. Every user-ID and related password is intended for the exclusive use of a specific individual. While user-IDs can be communicated in electronic mail messages and in other places, passwords must never be shared with anyone (IT support staff have their own access privileges and will never need to obtain a User’s password). A User may have more than one user-ID and password combination if access to multiple security systems is required for the Users assignments.

**User Authentication**

All production information system user-IDs must have an associated password or a stronger mechanism (such as a dynamic password token) to ensure that only the authorized User is able to utilize the user-ID. Users are responsible for all activity that takes place with their user-ID and password (or other authentication mechanism). Users must immediately change their password if they suspect that it has been discovered or used by another person.

Likewise, Users must notify the Help Desk if they suspect that these mechanisms have been compromised. User-IDs may not be utilized by anyone but the individuals to whom they have been issued. Users must not allow others to perform any activity with their user-IDs. Similarly, Users are forbidden from performing any activity with IDs belonging to other Users.


**PORTABLE COMPUTERS**

Portable, laptop, notebook, palmtop, and other transportable computers must not store, contain or utilize any confidential or sensitive information unless protected by the standard login process as described above. Users are responsible for the physical security of these devices and the protection of information stored on them.

**DATA**

Whenever non-public information is written to a floppy disk, magnetic tape, smart card, or other storage media, the storage media must be suitably marked with the highest relevant sensitivity classification. When not in use, this media must be stored in a secure location.

**REMOTE PRINTING**

Controls must be in place to prevent confidential or sensitive information from being viewed by unauthorized personnel. The User must ensure that confidential material is printed on a properly secured printer or one attended to by a person authorized to view the material.

**SHARING OR TRANSMISSION OF SECURE DATA**

Users must NOT establish electronic bulletin boards, local area networks, FTP servers, web servers, or modem connections to existing local area networks or other multi-user systems for communicating information without the specific approval of the ISO. Only designated Office of Information Services staff with special privileges may establish these types of services.

**DISPOSAL OF EQUIPMENT AND MEDIA**

Before computer storage media is sent to a vendor for trade-in, servicing, or disposal, all sensitive information must be destroyed or concealed according to methods approved by the Information Security Officer.

**PRIVILEGE SUSPENSION AND REVOCATION**

**General**

Information Owners establish access conventions for the revocation of User access privileges to the data they own. The Owner’s designee will use these conventions to grant and revoke User privileges on behalf of the Owner.

User Managers must promptly report all significant changes in a User’s duties or employment status that result in changes to access privileges using the computer account administration process. For all terminations, a designated organization such as Human Resources must also notify the ISO who will monitor the removal of User access to all data, information and systems to assure compliance.

User Managers must reevaluate the system privileges granted to Users every twelve (12) months. In the event that access requirements of the user have changed, the User
Manager must modify the User's access as detailed in the computer account administration process.

When a User leaves, both computer-resident files and paper/manual files must be promptly reviewed by his or her immediate manager to determine who should become the custodian of such files, and/or the appropriate methods to be used for file disposal. The User Manager must then promptly reassign the computer User's duties as well as specifically delegate responsibility for the files formerly assigned to that User.

User-IDs which have not seen any activity for a period of three months will have their privileges automatically revoked. Users who come back from an extended vacation, temporary reassignment or a leave of absence must have their manager reestablish their privileges.

**Session**
If there has been no activity on a workstation for twenty (20 minutes), the system must automatically blank the screen and suspend the session. Re-establishment of the session must take place only after the User has provided a valid password.

**Password Requirements**

*Difficult-To-Guess Passwords*
To minimize the likelihood of compromise, Users must choose passwords that are difficult to guess. This means that passwords must NOT be related to one's job or personal life. For example, a car license plate number, a child's name, job/hobby or fragments of an address must not be used. This also means passwords must not be a word found in the dictionary or some other part of speech. For example, proper names, places, technical terms, and slang must not be used.

*Easily Remembered Passwords*
Users should choose easily-remembered passwords that are at the same time difficult for unauthorized parties to guess:
- String several words together,
- Shift a word up, down, left or right one row on the keyboard,
- Bump characters in a word a certain number of letters up or down the alphabet,
- Transform a regular word according to a specific method, such as making every other letter a number reflecting its position in the word,
- Combine punctuation or numbers with a regular word,
- Create acronyms from words in a song or another known sequence of words,
- Deliberately misspell a word (but not a common misspelling), or
- Combine several preferences like hours of sleep desired and favorite colors.

*Repeated Password Patterns*
Users must not construct passwords with a basic sequence of characters that is then partially changed based on the date or some other predictable factor. For example, Users must NOT employ passwords like "JIM01JAN" in January, "JIM01FEB" in February, etc. Additionally, Users must not construct passwords that are identical or substantially similar to passwords they have previously employed.
Password Constraints
To ensure good password management, the following password standards must be implemented on all NYSDOT platforms when technically feasible:

- password must not be the same as the user-ID;
- password length minimum of eight (8) characters;
- strong passwords including alpha and numeric characters;
- maximum password age 90 days;
- minimum password age seven (7) days except for initial passwords which must be changed at the first logon;
- password uniqueness (history) - 12;
- lock out account after a specified number of failed log-on attempts - 6 invalid attempts;
- password lockout duration - forever, or until reset by an authorized person;

Password Management
Passwords, access control lists and other access control information must always be encrypted in storage or when transmitted over networks. Controls must be in place to prevent the unauthorized retrieval and use of stored passwords and access control information.

To allow passwords to be changed when needed, passwords must never be hard-coded (incorporated) into software or applications.

Initial passwords issued to a new User must be valid only for the new User's first on-line session. At that time, the User must be forced to choose another password. This same process applies to the resetting of passwords in the event that a User forgets a password.

All vendor-supplied default passwords must be changed before any computer or communications system is used. This procedure applies to passwords associated with end-user user-IDs, as well as passwords associated with system administrator and other privileged user-IDs.

Users must not share their individually assigned account password with anyone, including their manager or co-workers. Instead, Users must employ ISO approved, authorized mechanisms to share information such as local server shared directories, electronic mail, intranet pages, or floppy disks.

The display and printing of passwords must be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them.

Users are responsible for establishing passwords for all applications and systems software that comply with NYSDOT’s password standards.

Passwords must never be displayed in readable form outside a personal computer or workstation.

Password resets may only take place after the requester has been properly authenticated. The ISO must approve all methods of requester authentication and password communication. To obtain a new or changed password, a User must go through the prescribed authentication and password reset process. After the password has been reset, the User must log in and change the password at the first opportunity.
After a password has been changed, an email notification must be sent to the User. The User must contact Information Security immediately if the reset was not initiated by the User.

**SYSTEM DEVELOPMENT**

The following standards prevent access to production data by unauthorized personnel and improve the integrity of applications.

**Separation between Production, Development, and Test Systems**
There shall be a separation between the production, development, and test environments. This will ensure that security is maintained in a much more rigorous way for the production system. Development and test staff are not normally permitted to have access to production systems. Only Information Owners can approve access to production data to developers. Likewise, all production software testing must proceed with sanitized information (where sensitive information is replaced with dummy data). A formal and documented change control process must also be used to restrict and approve changes to production systems and information.

**Application Development**
Prior to moving software to production status, programmers and other technical staff must remove all special access paths so that access may only be obtained via normal secured channels. This means that all trap doors and other short-cuts that could be used to compromise security must be removed. Likewise, all system privileges needed for development efforts, but not required for normal production activities, must be removed.

All the User-level and administrative-level access controls required by information security policies and procedures must be established and enabled before production information systems can be placed into operation.

**Migration Control**
A methodology must be implemented for an orderly and controlled migration of software from the development environment, through the test environment and ultimately to the production platforms. Application development staff must not have the ability to move any software directly into the production processing environment. Controls must be in place to prevent the migration of unauthorized application code into the production environment.

System privileges allowing the modification of production business information must be restricted to production applications. Privileges must be established such that system Users are not able to modify production data in an unrestricted manner. Users may only modify production data in predefined ways that preserve or enhance its integrity. Updates to production databases must only be made through established channels which have been approved by management. The use of direct database access utilities in the production environment is not permitted because these programs will circumvent database synchronization and replication routines, input error checking routines, and other important control measures.
**LOGS AND OTHER SECURITY TOOLS**

Computer and communications systems handling sensitive or critical information must securely log all significant security relevant events. Examples of security relevant events include: Users switching user-IDs during an on-line session, attempts to guess passwords, attempts to use privileges that have not been authorized, modification of production application software, modifications to system software, changes to User privileges, and changes to logging subsystems.

The ISO will prepare regular reports for management regarding security access issues, incidents, status, degree of compliance, changes and initiatives and other relevant events.

**REPORTING PROBLEMS**

**What to Report**
Any security incidents including unauthorized access or attempts, theft or disclosure of passwords or access controls, any loss, alteration or suspected disclosure of data or any violation of security policies, procedures and standards must be promptly reported to the NYSDOT Help Desk.

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

**IV. RELATED AUTHORITATIVE SOURCES**

**NYS**
New York State Information Security Policy – Cyber Security Policy P03-002

**NYSDOT**
- Information Security Policy, MAP 2.18.2.0
- Non-Disclosure Procedure, MAP 2.18.2.4
- Information Security Roles and Responsibilities Policy, MAP 2.18.2.5
- Privileged Access Procedure, MAP 2.18.2.8
- Disciplinary Procedure, MAP 4.8-2
- Removal of Computer Accounts, Bulletin B-04-G 042
- Connecting to the NYSDOT Network, Bulletin B-04-G 053
- Password Security, Bulletin B-05-G 175