DEPARTMENT OF CIVIL SERVICE
INFORMATION SECURITY POLICY

OCTOBER 1, 2007

Nancy Groenwegen
Commissioner

LIST OF POLICIES

Policy Name	INFORMATION SECURITY POLICY PURPOSE
Category	Security
Policy Number	1.01
Policy Owner	Information Security Officer (ISO)
Policy Level	Department
Effective Date	October 1, 2007
Revision Date	October 1, 2008

PURPOSE

To establish the purpose of the Department of Civil Service Information Security Policy.

POLICY STATEMENT

The Department of Civil Service (DCS) Information Security Policy implements the New York State policy issued by the Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) and the HIPAA security requirements; and is a collection of over twenty security policies. The purpose of the Information Security Policy is to define a set of minimum security requirements that must be met by the Department.

The primary objectives of the Information Security Policy are to:

1. effectively manage the risk of security exposure or compromise within Department systems;
2. communicate the responsibilities for the protection of Department information;
3. establish a secure processing base and a stable processing environment;
4. to the extent reasonably possible, reduce the opportunity for errors to be entered into an electronic system supporting Department business processes;
5. preserve management's options in the event of an information asset misuse, loss or unauthorized disclosure; and
6. promote and increase the awareness of information security.

The policy applies to all workforce members, business partners, clients, and suppliers.

Where conflicts exist between this policy and Division policies, the more stringent policy takes precedence.

DEFINITIONS

Workforce Member: staff, contractor, volunteer, intern working for or on behalf of the Department of Civil Service.

REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA), Security Regulation, Privacy and Security Regulation
- New York State Cyber Security Policy P03-002
- Information technology – Code of practice for information security management, ISO/IEC 17799

Policy Name	INFORMATION SECURITY PROGRAM SCOPE
Category	Security
Policy Number	1.02
Policy Owner	Information Security Officer (ISO)
Policy Level	Department
Effective Date	October 1, 2007
Revision Date	October 1, 2008

PURPOSE

To establish the scope of the Department of Civil Service Information Security Program.

POLICY STATEMENT

All Department information must be protected from unauthorized access to help ensure the information's confidentiality and maintain its integrity. The Department has established an information security function led by the ISO. The scope of the Information Security Program is to:

1. develop, deploy and maintain an information security architecture that will provide security policies, mechanisms, processes, standards and procedures that meet current and future business needs of the Department;
2. provide information security consulting to the Department regarding security threats that could affect the computing and business operations, and make recommendations to mitigate the risks associated with these threats;
3. assist management in the implementation of security measures that meet the business needs;
4. develop and implement security training and awareness programs that educate workforce members and vendors with regard to the information security requirements;
5. investigate and report to management breaches of security controls, and implement additional compensating controls when necessary to help ensure security safeguards are maintained;
6. participate in the development, implementation and maintenance of disaster recovery processes and techniques to ensure the continuity of the Department's business, in the event of an extended period of computing resource unavailability;

The Information Security Program will address all information, regardless of the form or format, which is created or used in support of business activities.

The Security program will contain protocols and procedures that support the implementation of the information security policy for systems and technologies being used within their domains. These security protocols and procedures will be produced and implemented to ensure uniformity of information protection and security management across the different technologies deployed within the Department. The protocols and procedures can be used as a basis for policy compliance measurement.

DEFINITIONS

Availability: The property of being operational, accessible, functional and usable upon demand by an authorized entity, e.g. a system or user.
Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Integrity: The property that data has not been altered or destroyed from its intended form or content in an unintentional or an unauthorized manner.
Workforce Member: staff, contractor, volunteer, intern working for or on behalf of the Department of Civil Service.

REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA), Security Regulation, Privacy and Security Regulation
- New York State Cyber Security Policy P03-002
- Information technology – Code of practice for information security management, ISO/IEC 17799

Policy Name	INFORMATION SECURITY ORGANIZATION AND RESPONSIBILITIES
Category	Security
Policy Number	1.03
Policy Owner	Information Security Officer (ISO)
Policy Level	Department
Effective Date	October 1, 2007
Revision Date	October 1, 2008

PURPOSE

To establish the Department of Civil Service Information Security Organization roles and responsibilities.

POLICY STATEMENT

The Commissioner will establish the framework for the Department of Civil Service Information Security Program and appoint an ISO.

The ISO is responsible for the implementation, enhancement, monitoring, and enforcement of the information security policy and protocols of all stored, processed, or transmitted data. The ISO may delegate these responsibilities to others, at the same time ensuring the duties are completed with due diligence. The ISO's responsibilities include:

- Directing the Information Security Program
- Chairing the Information Security Steering Committee
- Producing recommendations for policy, protocols, and processes
- Educating workforce members
- Implementing appropriate safeguards
- Facilitating compliance with safeguards
- Investigating alleged incidents
- Participating in the development, implementation and maintenance of disaster recovery programs
- Reporting on security program activities
- Supporting statewide security initiatives
- Evaluating new threats and counter measures
- Reviewing and approving all external connections to the network
- Providing consulting to all levels of management on information security
- Following New York State cyber-incident reporting requirements
- Being aware of the laws and regulations affecting security controls
- Reporting information security program compliance to the Commissioner

The Information Security Steering Committee include, at a minimum, Office of Human Resources Management, Office of Financial Management, Director of Internal Audit, Information Resource Management (IRM), and Office of the Counsel. The Information Security Steering

Committee will meet regularly. The responsibilities of the Information Security Steering Committee include:

- Developing the Department's information security strategy
- Overseeing the Department of Civil Service Information Security Program
- Formulating the security policies, protocols, and standards

- The responsibilities of the members of the Information Security Team include:
- Assisting in developing and communicating the Information Security Policy, protocols, standards for the Department
- Identifying security awareness issues
- Assisting Division Directors with the development of awareness materials and tools
- Monitoring the effectiveness of information security measures
- Conducting security reviews and identifying the need for additional controls
- Participating in security incident response teams
- Providing support to new application and system development, acquisition and deployment
- Assessing security risks
- Developing the access control strategy, firewall strategy, network deployment strategy, audit control strategy, and other security strategies as identified in the risk assessment
- Facilitate security planning meetings with various members of Technical Support, the ISO, the CIO, and others as appropriate

- Division Directors/Information Owners have the accountability for all of the security safeguards regarding their information asset. The responsibilities of the Division Director/Information Owner include:

- Classifying information assets
- Ensuring consistent labeling and handling of information assets
- Periodically reviewing security measures for information assets
- Handling requests for information regarding the information assets
- Ensuring security controls for third party access to the information asset
- Assigning and supervising data custodians
- Ensuring regulatory compliance
- Implementing Department and Division policies
- Ensuring adequate controls for the information assets
- Establishing access privileges for the information assets
- Ensuring that Division workforce members are informed of the security policies and understand their security responsibilities
- Establishing and maintaining business continuity plans for their Division
- Coordinating with the Division Liaison regarding issues related to IRM efforts

- The responsibilities of IRM include:
- Implementing appropriate security controls in accordance with the Policies
- Using their privileged access to information systems only as authorized
- Responding quickly to suspected security incidents and escalating them in accordance with Security Incident Response Guidelines
- Reporting information security related activity to the ISO
- Creating a security team or appointing security analysts or security administrators to handle the tasks that support ISO goals.

- Ensuring processes, policies, and requirements are identified and implemented relative to security requirements of the Division Directors/Information Owners.
- Ensuring the proper controls of information are implemented.
- Ensuring the participation of the ISO and Information Security Team in identifying and selecting security controls and procedures.
- Ensuring that critical data and recovery plans are backed up and kept at a secure off site facility.

Workforce members are responsible for understanding of their role in the security of the Department's computing resources and information assets. They are responsible for gaining a clear understanding of what uses are acceptable and what uses are unacceptable. They must understand and adhere to all security policies, actively report suspected security incidents, report misclassification of information, and actively protect all information and resources. All workforce members are responsible for reading, understanding, and signing the security policies appropriate to their position, which includes at a minimum, the *Acceptable Use Policy*.

Refer to *Acceptable Use Policy, Security Incident Response Management Policy,* and *Contingency Planning Policy.*

DEFINITIONS

Data Custodian: The individual appointed by the Division Director/Information Owner to make decisions on their behalf.
Information Asset: All categories of information, including but not limited to: records, files, and databases.
Information Owner: The Division Director that has responsibility for making classification and control decisions regarding use of information assets.
Workforce Member: Staff, contractor, volunteer, intern working for or on behalf of the Department of Civil Service.

REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA), Security Regulation, Privacy and Security Regulation
- New York State Cyber Security Policy P03-002
- Information technology – Code of practice for information security management, ISO/IEC 17799

Policy Name	DATA CLASSIFICATION
Category	Security
Policy Number	1.04
Policy Owner	Information Security Officer (ISO)
Policy Level	Department
Effective Date	October 1, 2005
Revision Date	October 1, 2006

PURPOSE

To properly manage all Department information from its creation, through authorized use, to proper disposal.

POLICY STATEMENT

In order to ensure that all Department information is properly managed from its creation, through authorized use, to proper disposal, each information asset must be defined and classified based on its value, sensitivity, consequences of loss or compromise, and/or legal and retention requirements. Each classification will have a set or range of controls, designed to provide the appropriate level of protection of the information and its associated application software commensurate with the value of the information in that classification. Security controls will include considerations regarding identification and authentication, access control, confidentiality, network security, host security, physical security, data integrity, non-repudiation, monitoring and compliance.

All information must have a designated information owner. Division Directors/Information Owners are responsible for classifying all information.

The Division Director/Information Owner will be responsible for assigning the initial information classification, making all decisions regarding security controls, and making daily decisions regarding information management. Division Directors/Information Owners must conduct periodic high-level business impact analyses on the information to determine its relative value and risk of compromise. Based on the results of the assessment, the Division Directors/Information Owners must reclassify the information.

Data sensitivity will be established by assigning levels of confidentiality, integrity, and availability to each information asset. Additional information must be associated with each information asset regarding retention requirements, location, current access control measures, ease of recovery, and other legal requirements governing the handling of the information asset. When making such decisions the information "owner" must consider the external regulatory issues surrounding the data's classification, particularly those surrounding the Freedom of Information Law (FOIL) and the Health Insurance Portability and Accountability Act (HIPAA).

Ratings for confidentiality, integrity, and availability are to follow these definitions:

Confidentiality

- Confidential (High)
  - Unauthorized or unintentional disclosure of the information asset could result in grave loss of public confidence, in fraud, in major legal action, or in major financial loss.

- Internal (Medium)
  - Unauthorized disclosure of the information asset could compromise the Department enough to result in significant financial loss or legal action.
- Public (Low)
  - Unauthorized or unintentional disclosure of the information asset would result in only public relations issues and minor to no financial loss.

Integrity

- High
  - Unauthorized or unintentional modification of the information asset could result in grave loss of public confidence, in fraud, in major legal action, or in major financial loss.
- Medium
  - Unauthorized or unintentional modification of the information asset could compromise the Department enough to result in significant financial loss or legal action.
- Low
  - Unauthorized or unintentional modification of the information asset would result in only minor financial loss and would require only administrative action to correct.

Availability

- High
  - The loss of the information asset could result in grave loss of public confidence, major financial loss or major legal action.
- Medium
  - The lack of the information asset results in a serious compromise of a business function or a likelihood of significant financial loss or legal action.
- Low
  - The business function can continue without the information asset, or
  - The loss of the information asset will result in only minor financial loss.

DEFINITIONS

Data Custodian: The individual appointed by the Division Director/Information Owner to make decisions on their behalf.
Information Asset: All categories of information, including but not limited to: records, files, and databases.
Information Owner: The Division Director that has responsibility for making classification and control decisions regarding use of information assets.

REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA), Security Regulation, Privacy and Security Regulation
- New York State Cyber Security Policy P03-002
- Information technology – Code of practice for information security management, ISO/IEC 17799

Policy Name	ACCEPTABLE USE
Category	Security
Policy Number	1.05
Policy Owner	Information Security Officer (ISO)
Policy Level	Department
Effective Date	October 1, 2007
Revision Date	October 1, 2008

PURPOSE

To identify acceptable use and non-acceptable use of the Department of Civil Service's computing resources and information assets, to set expectations regarding privacy while using the Department's email and Internet services, to explain Department rights, to address enforcement and violations provisions, and to set forth the Department's *Acceptable Use Policy* that all Department workforce members are required to read and sign.

POLICY STATEMENT

The use of the Department's computing resources and information assets by any workforce member must be consistent with this *Acceptable Use Policy*. All workforce members must follow this policy at all times while using Department computing resources and information assets. Any misuse of the Department's resources may result in disciplinary action including termination of employment. All workforce members must understand and sign a copy of this *Acceptable Use Policy*.

The Department provides computing resources, information, and technical support to workforce members for Department business purposes only. Personal and casual use is permitted and must be kept to a minimum.

Workforce members must:

- Conduct computer processing activities only within the limits of the access assigned or delegated by management and to inform management of situations necessitating a change in access levels.
- Take required actions to protect information and computing resources from unlawful, unauthorized, or unacceptable actions or events resulting in modification or destruction.
- Be personally accountable for the use and safekeeping of access codes, passwords, keys, or other means used to secure access to computing resources.
- Observe all contractual, regulatory, and legal obligations governing the use of Department information and facilities. Workforce members must comply with all software licenses, copyrights, patent, trade secret, and any state, federal, and international laws governing intellectual property.
- Report suspected security breaches promptly to the attention of management and/or the ISO.

Workforce members must not:

- Disable utilities including anti-virus software installed on their workstations or other computing resources and may not alter computing hardware, software or configurations provided by the Department;

- Install a wireless network or wireless access point and may not download software or utilities;
- Connect dial-up modems to the Department's computer systems connected to a Department local area network or to another internal communication network;
- Store data to local drives unless authorized; or
- Intentionally damage or alter the Department's information assets.

Public Web Site

Workforce members preparing public web site content must be compliant with copyright laws, Department policy, and Department protocols. All content posted on the public web site must be reviewed and approved the ISO or security designee.

Internet Access and Electronic Mail

Internet access and electronic mail (email) are to be used primarily for authorized activities based upon business need. Personal and casual use is permitted and must be kept to a minimum. Internet access is only authorized through the use of an appropriately configured browser as distributed by IRM technical support. Other methods of accessing the Internet using the Department systems are prohibited.

Workforce members are prohibited from using their Internet access in any manner that violates the law or Department policy. Material that is fraudulent, harassing, embarrassing, intimidating, profane, or otherwise unlawful or inappropriate may not be created, maintained, transmitted, displayed, downloaded, or stored on Department computing resources nor disseminated through the email system. Unacceptable use includes, but is not limited to, the use of computing resources:

- To represent yourself as someone else;
- For sending unsolicited email to persons with whom you do not have a relationship, or without the express permission of your manager;
- For unauthorized attempts to break into any computing system whether the Department's or another organization's;
- For theft or unauthorized copying of electronic files;
- For posting sensitive Department information without authorization from Department;
- To interfere with or disrupt network users, services or equipment;
- For any activity which can create a denial of service, such as "chain letters";
- For "sniffing" or monitoring network traffic;
- For personal gain;
- For representing personal opinions as those of the Department or New York State;
- For solicitation for religious and political causes;
- For private advertising of products or services;
- For marketing or business transactions;
- For harm against any person or entity; and
- To degrade, harass, or embarrass workforce members, other individuals, or groups.

The Department's Internet services are provided on an as is, as available basis. The Department makes no warranties, express or implied, with respect to Internet service, and it specifically assumes no responsibilities for:

- The content of any advice or information received by a workforce member via the Internet or any costs or charges incurred as a result of seeking or accepting such advice;

- Any costs, liabilities or damages caused by the way the workforce member chooses to use his/her agency Internet access;
- Any consequence of service interruptions or changes, even if these disruptions arise from circumstances under the control of the Department.

Workforce members must never set automatic forwarding of email to their personal email accounts unless authorized. Workforce members should anticipate regular automatic deletion of email in inboxes and should take measures to retain email accordingly.

Phishing is a scam in which an email message directs the email recipient to click on a link that takes them to a web site where they are prompted for personal information such as a pin number, social security number, bank account number or credit card number. Both the link and web site may closely resemble an authentic web site however, they are not legitimate. If the phishing scam is successful, personal accounts may be accessed. Workforce members must follow these rules if they receive one of these emails:

- Do not click on the link. In some cases, doing so may cause malicious software to be downloaded to your computer.
- Delete the email message.
- Do not provide any personal information in response to any email if you are not the initiator of the request.

Electronic Devices and Removable Media

Electronic devices must not be attached to a DCS PC unless the device has been issued by DCS and the use has been approved by the ISO. Once approved, electronic devices must always be secured and locked at the desk. Removable media, such as floppies and CD's must be issued by DCS, must be encrypted and must not be discarded via the trash. Workforce members must place discarded removable media in the security scrap box/container for removable media.

When mobile computing facilities such as notebooks, PDA's, blackberries, laptops and mobile phones are used in public places, care must be taken to avoid the risk of unauthorized persons viewing information on the screen. Such equipment must not be left unattended, must be physically locked when not in use, must be encrypted, and must be configured with a password supplied by the Help Desk to enable the equipment to function. All personal, private or sensitive business information (PPSI) must be stored only in encrypted form, and only on external (removable) storage media supplied by the Help Desk. No such information is to be stored on any internal (non-removable) storage devices.

Workforce members in the possession of portable, laptop, notebook, PDA's, blackberries, and other transportable computers must not check these computers in airline luggage systems. These computers must remain in the possession of the traveler as hand luggage unless other arrangements are required by federal or state authorities.

If using telephones outside the Department for business reasons, workforce members should take care that they are not overheard when discussing sensitive or confidential matters, avoid use of any wireless or cellular phones when discussing sensitive or confidential information, and avoid leaving sensitive or confidential messages on voicemail systems. Workforce members must not disclose non-public Department information over an instant messaging, electronic team-room or conferencing system. If sensitive or confidential information will be discussed during a teleconference, workforce members must not send teleconference call-in numbers and pass-codes to a pager.

Clear Desk

At the end of the workday, workforce members must clear their desk of sensitive material. When away from the desk for any length of time, removable media with personal, private or sensitive information (PPSI) must be secured.

Faxing and Printing

Workforce members must not use Internet fax services to send or receive PPSI, must not use third party fax services to send or receive PPSI, and must not send PPSI via wireless fax devices. If sending PPSI documents via fax, workforce members are to verify the phone number of the destination fax and contact the recipient to ensure protection of the fax either by having it picked up promptly or by ensuring that the fax output is in a secure area. When printing a document with PPSI, the document must be picked up immediately.

Passwords

Workforce members must follow password best practices whenever technology permits. These password best practices include but are not limited to:

- Do not write down passwords;
- Use passwords that are not easily guessed or subject to disclosure through a dictionary attack;
- Keep passwords confidential and do not share individual passwords with another individual;
- Change passwords at regular intervals;
- Change temporary passwords at the first logon;
- When technology permits, passwords should contain a mix of alphabetic, numeric, special, and upper/lower case characters; and
- Do not include passwords in any automated logon process, e.g., stored in a macro or function key, web browser or in application code.
- Whenever you leave your desk, press ctrl-alt-delete to lock your computer.

When Working From a Remote Location

Working from a remote location must not occur unless first authorized by the Department. Once approved by the Department, workforce members must ensure that, at a minimum, the following security controls are in place at the remote location:

- PPSI must not be in view of family, friends, or other guests at the home or remote location.
- Passwords must not be written down nor kept in visible locations at the remote location or home.
- Files, printed documents, external storage devices with PPSI must be secured.
- When transporting PPSI, such as files, printed documents, and external storage devices, in a car, these items must be secured.
- All external storage devices must be encrypted.
- Encryption keys must not be stored with external storage devices.
- Paper or media with PPSI must not be discarded at home but must be brought back to the site and disposed via the security scrap mechanisms provided by the Department.
- Home computers used for work must have current anti-virus software, a method for maintaining current signature files, and an active firewall.

Reporting Incidents

Each workforce member must understand his/her role and responsibilities regarding information security issues and protecting the Department's information. Workforce members are required to report any observed or suspected incidents to a manager and/or the ISO or security designee immediately. Workforce members must not attempt to prove a suspected weakness or incident.

Examples of suspected security incidents are:

1. Unsecured computing resources
2. Any unsupervised or otherwise unauthorized person in a server area or a protected area
3. Release of internal directories or other documentation that provides locations of server areas
4. Attempts by an unauthorized individual to obtain access credentials, e.g., ID badges, security access codes, keys.
5. Unauthorized attempts to gain access to DCS network systems or facilities
6. Unapproved hardware connected to the DCS network
7. Computer hardware left in an unsecured area
8. A potential fire or water hazard
9. Damaged equipment, facilities or utilities
10. Loss or misplacement of media (e.g. disks, tapes, paper) containing PPSI that has not been encrypted
11. Inappropriate use of the computing environment
12. Disclosure of PPSI

Reporting Computer Problems

Workforce members are to contact the Help Desk if they notice that their machine is compromised. Possible symptoms of a compromised computer are if the machine is:

- Slow or non-responsive
- Running programs that aren't expected
- Showing signs of high level of activity to the hard drive that is not the result of anything that was initiated by the user
- Displaying messages on the screen that the user hasn't seen before
- Running out of disk space unexpectedly
- Unable to run a program because of lack of memory – and this doesn't happen normally
- Rejecting a valid and correctly entered password

Management

Division Directors and Managers are accountable for enforcing this policy and reporting incidents to the ISO.

Monitoring of Workforce Member Activity

Workforce members should not have an expectation of privacy in anything they create, store, send, or receive on the Department's computing resources. The Department may monitor any and all aspects of its computer systems, including, but not limited to sites visited by workforce members on the Internet, chat groups or newsgroups, material downloaded or uploaded by workforce members to the Internet, or email sent and received by workforce members. The Department conducts content filtering of all Internet activity and outbound and inbound email.

Inspection, monitoring, or reviewing may be done as part of an investigation into allegations of misconduct, fraud, or other wrongdoing; for technical or maintenance purposes; to assure system security; to comply with Department policy and/or legal requirements; or for training purposes. Notifying workforce members that their electronically stored files or communications are being examined will occur optionally at the Department's discretion.

Department of Civil Service Rights

Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510 et seq), notice is hereby given that there are no facilities provided by this system for sending or receiving private or confidential electronic communications. The Department has access to all access attempts, messages created and received, and information created or stored using the Department's resources, and will monitor use as necessary to assure efficient performance and appropriate use. Information relating to or in support of illegal activities will be reported to the appropriate authorities.

The Department reserves the right to log and monitor use. The Department reserves the right to remove a user account from the network. The Department assumes no responsibility or liability for files or information deleted.

The Department will not be responsible for any damages. This includes the loss of data resulting from delays, non-deliveries, or service interruptions caused by negligence, errors or omissions. Use of any information obtained is at the user's risk. The Department makes no warranties, either express or implied, with regard to software obtained from the internet.

The Department makes no warranties, express or implied, with respect to Internet service, and it specifically assumes no responsibilities for:

- The content of any advice or information received by a user outside NYS or any costs or charges incurred as a result of seeking or accepting such advice;
- Any costs, liabilities or damages caused by the way the user chooses to use his/her agency Internet access;
- Any consequence of service interruptions or changes, even if these disruptions arise from circumstances under the control of the Department. The Department's Internet services are provided on an as is, as available basis.

Clear violations of this policy will result in disciplinary actions as appropriate. The Department reserves the right to change its policies and rules at any time.

DEFINITIONS

Electronic devices: Electronically controlled devices that store data, run programs, execute commands, or transmit information. Electronic devices include but are not limited to USB port memory sticks, laptops, personal digital assistants (PDA), and camera phones.
Information Asset: All categories of information, including but not limited to: records, files, and databases.
Local Drive: A storage drive or device that is connected to one's local computer, rather than on a network server managed by IRM.
PPSI: Personal, private or sensitive information.
Remote Access: computing device access from outside the Department's private, trusted network. This access includes modem dial up, web access to applications, and direct connections with remote organizations.

Workforce Member: Staff, contractor, volunteer, intern working for or on behalf of the Department of Civil Service.

REFERENCES

- Electronic Communications Privacy Act of 1986 (18 USC 2510 et seq).
- Health Insurance Portability and Accountability Act (HIPAA), Security Regulation, Privacy and Security Regulation.
- New York State Cyber Security Policy P03-002.
- Information technology – Code of practice for information security management, ISO/IEC 17799.

State of New York
Department of Civil Service
Alfred E. Smith Building
Albany, New York 12236

OFFICE OF HUMAN RESOURCE MANAGEMENT
Acceptable Use Policy Signature Page

ADM-240 (6/05L)

I have read and understand the Acceptable Use Policy, Security Policy 1.05, dated October 1, 2007 that outlines the rights, responsibilities and governance of DCS computing resources and information assets.

I understand that I must do certain things to protect the Department's data and systems. For example, I understand that I am to lock away any floppies that I use when I am away from my desk, lock my computer when I am away from my desk, clear my desk of sensitive material at the end of the day, and report security incidents.

I understand that there are actions that I must **not** take as well. For example, I understand that I must not install programs or change programs already installed on my computer, plug in a piece of equipment to my computer, or disclose my password to others.

I understand that the Department can monitor my actions. I have had the opportunity to ask questions.

I have read and understand this *Acceptable Use Policy*:

Workforce Member's Signature			**Date**
Workforce Member's Name (print)			
Division/Unit			
Telephone Number	–	–	**Ext.**

Please sign and return this page to Office of Human Resources Management. This page will be filed in your personal history folder. Keep the policy for your use. Please do not hesitate to ask questions to clarify items in this policy.

Policy Name	SECURITY AWARENESS
Category	Security
Policy Number	1.06
Policy Owner	Information Security Officer (ISO)
Policy Level	Department
Effective Date	October 1, 2007
Revision Date	October 1, 2008
Replaces	

PURPOSE

To ensure that workforce members are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their work.

POLICY STATEMENT

An information security awareness program that addresses the needs of all DCS workforce members must be developed, implemented and maintained. The program will include supplements to the new employee orientation program. When appropriate, the training will be role specific. The program must address security procedures, the workforce member's role and responsibilities regarding the protection of DCS's information assets, and the proper use of its computing resources and facilities. At a minimum, security awareness training must be reinforced annually.

All workforce members must complete the assigned information security awareness training. Division Directors/Information Owners must identify any information security awareness or training needs that arise in their Division. Division Directors must ensure that all Division workforce members complete the assigned information security awareness training, according to the prescribed security awareness program. The ISO will oversee the design and deployment of the information security awareness training. The Information Security Team and the Planning and Training Unit will collaborate in the design and deployment of the awareness program.

DEFINITIONS

Information Asset: All categories of information, including but not limited to: records, files, and databases.
Information Owner: The Division Director that has responsibility for making classification and control decisions regarding use of information assets.
Workforce Member: Staff, contractor, volunteer, intern working for or on behalf of the Department of Civil Service.

REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA), Security Regulation, Privacy and Security Regulation
- New York State Cyber Security Policy P03-002

- Information technology – Code of practice for information security management, ISO/IEC 17799

Policy Name	PHYSICAL SECURITY
Category	Security
Policy Number	1.07
Policy Owner	Information Security Officer (ISO)
Policy Level	Department
Effective Date	October 1, 2007
Revision Date	October 1, 2008

PURPOSE

To prevent physical breaches to the Department's computing resources and information assets.

POLICY STATEMENT

Critical or sensitive business information processing facilities should be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls. They must be physically protected from unauthorized access, damage and interference. The protection provided must be commensurate with the identified risks in the ongoing risk assessment.

Physical barriers must be established around the Department's premises and information processing facilities and facility access controls must be implemented. Access rights for all workforce members must be based on the workforce member's function and must be approved by the Division Director. Access rights should be reviewed and updated regularly. All workforce members must wear Department-issued visible identification. All visitors entering and exiting the building must be supervised or cleared and a record of the visit should be maintained. Workforce members must inquire about the location or activities of any unsupervised non-workforce member in the building. Unexplained activity of any kind must be reported.

All site or building digital access must be disabled immediately upon termination, resignation, or separation from a project, keys or key cards must be collected, and access codes must be changed.

All networking and server resources, whether it be in production, in development, or stored, must be secured in designated secure areas that are locked and either alarmed or monitored. Equipment receiving and distributing procedures should include a registration process and documentation of the personnel receiving and distributing the equipment. The receiving process for equipment must include a central holding and receiving area where incoming equipment can be inspected before moving it to the point of use. The external door(s) of a holding area should be secured when the internal door is opened. Equipment that is not expected must be turned away and not received. On receipt of all equipment, all appropriate inventories must be updated in a timely manner.

All doors to computer rooms must be fire doors and should slam shut. Barriers or walls securing computer rooms must be extended from real floor to real ceiling to prevent unauthorized entry and environmental contamination such as that caused by fire and flooding. Windows throughout the building must be locked and must not be opened. Computer rooms must have up-to-date fire protection. Computer rooms must be located on or above the ground floor. Consideration must

also be given to any security threats presented by neighboring premises, for example, leakage of water from other areas. Equipment must be protected from power failures and other electrical anomalies. Options to achieve continuity of power supplies can be selected based on the risk assessment and business need. Emergency lighting must be provided in case of main power failure. Cabling carrying data or supporting information services should have protective controls commensurate with the risk.

All computing equipment must be raised off of the floor at all times. When closets, drawers, or shelves are used to house production or in development networking equipment, these structures must be secured. Power switches to production servers must be protected from unauthorized and accidental access. All source media for production servers, applications and license keys must be clearly labeled and stored in a secured area. Photographic, video, audio or other recording equipment should not be allowed in server rooms unless authorized. Hazardous or combustible materials should be stored securely at a safe distance from any computing resource. Refer to *Media Handling and Disposal Policy* regarding equipment moves and disposal.

All computing equipment must be maintained in accordance with the supplier's recommended service intervals and specifications to ensure its continued availability and integrity. Only IRM may repair or service computers and records must be kept of all suspected or actual faults and all preventive and corrective maintenance.

All workforce members are involved in the physical security of the Department's security perimeters. Workforce members must not disable or circumvent physical security measures in any manner. These controls must be evaluated annually, during planning stages that may change physical security, or whenever the physical environment changes.

Clear screen technology must be used on all Department workstation screens. Workstation screens that display personal, private or sensitive information (PPSI) must be out of view of public areas. Sensitive material, computer screens, and security scrap deposit boxes must not be placed in an unsupervised common walkway. At the end of the day, workforce members must clear their desk of sensitive material.

Secure faxing procedures must be deployed to secure sensitive faxes that are either being received or being sent. Fax machines that receive or send sensitive information must be positioned out of the line of traffic of both clients and workforce members. Workforce members must retrieve sensitive print and/or faxes immediately upon printing. Access to electronic team-rooms that share sensitive information shall be limited. When working remotely, specific controls are required. Refer to *Acceptable Use Policy* regarding physical security measures when working remotely and when traveling.

Facility repairs relating to physical access must be repaired immediately. If a delay is necessary, additional physical security controls must be established for the time period. All repairs to the building must be supervised and documented. No repair work may occur that is outside of written scope definitions.

DEFINITIONS

Clear screen technology: technology that automatically clears the computer screen based on inactivity.

Electronic team-room: a computer-based multi-user data communication service.

Information Asset: All categories of information, including but not limited to: records, files, and databases.
Workforce Member: Staff, contractor, volunteer, intern working for or on behalf of the Department of Civil Service.

REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA), Security Regulation, Privacy and Security Regulation
- New York State Cyber Security Policy P03-002
- Information technology – Code of practice for information security management, ISO/IEC 17799

Policy Name	ACCESS CONTROL
Category	Security
Policy Number	1.08
Policy Owner	Information Security Officer (ISO)
Policy Level	Department
Effective Date	October 1, 2007
Revision Date	October 1, 2008

PURPOSE

To control access to information systems.

POLICY STATEMENT

The Department's information assets will be protected by logical and physical access control mechanisms commensurate with the value, sensitivity, consequences of loss or compromise, legal requirements and ease of recovery of these assets as identified by the Division Director/Information Owner. Division Directors/Information Owners are responsible for determining who should have access to protected resources within their jurisdiction and what those access privileges will be. These access privileges will be granted in accordance with the user's job responsibilities.

All access methods to the Department's trusted internal network must require all authorized users to authenticate themselves through use of an individually assigned user-ID and an authentication mechanism. Network controls must be developed and implemented that ensure that an authorized user can access only those network resources and services necessary to perform their assigned job responsibilities. Passwords must not be stored in clear text.

Logon banners must be implemented on all systems where that feature exists to inform all users that the system is for Department of Civil Service business or other approved use, and that user activities may be monitored.

When accessing the DCS network remotely, identification and authentication of the entity requesting access must be performed in such a manner as to not disclose the password or other authentication information that could be intercepted.

All remote connections to a computer must be made through managed central points-of-entry. Exceptions require a review by the Information Security Team and a waiver signed by the ISO. In the special case where a server, storage device or other computer equipment has the capability to automatically connect to a vendor to report problems or suspected problems, the review must ensure that connectivity is encrypted and does not compromise the DCS network or other third party connections. Third parties with connections must sign and process a *Third Party Connection and Data Exchange Agreement* with DCS. Every Third Party user must sign a *Third Party Acceptable Use Policy and Agreement.* Refer to *Third Party Connection and Data Exchange Policy* and *Remote Access Policy*.

Access to operating system code, services and commands is restricted to only those individuals for whom such access is necessary in the normal performance of their job responsibilities. All individuals requiring enhanced privileges must be provided with a unique privileged account for their sole use. Usernames must not give any indication of the user's privilege level. If privileged account holders are required to perform business transactions, they must use a second user-ID. Passwords to privileged accounts must not be shared with others unless specific authorization has been given.

In certain circumstances, where there is a clear business requirement or a system limitation, the use of a shared user-ID and password for a group of users or a specific job can be used. Approval by the ISO should be documented in these cases and additional compensatory controls must be implemented to ensure that accountability is maintained.

Where technically feasible, default administrator accounts must be renamed, removed or disabled. The default passwords for these accounts must be changed if the account is retained, even if the account is renamed or disabled.

Access to Department business and systems applications must be restricted to those individuals who have a business need to access those applications or systems in the performance of their job responsibilities. Access to source code for applications and systems must be restricted and additional controls must be placed on this type of access.

Networks will have sufficient controls to maintain a trusted internal network and ensure protection of the services connected to these networks. At a minimum this will contain:

1. Separation of operational responsibility for the networks from computer operations, where practical.
2. Separation of the administration of security from other system administrator roles, where practical.
3. Remote use procedures.
4. Safeguards for data passing across borders to public networks.

Electronic devices must not be attached to a DCS PC unless the use has been approved by the ISO.

Any electronic signature usage and any use of a public key infrastructure (PKI) shall comply with applicable laws and regulations.

Cryptographic controls must be used to protect sensitive information during transmission. A secure environment for controlling cryptographic keys must be created by IRM.

Protocols on network planning, analysis, controls, and deployments must be developed and maintained in a current state by the Information Security Team. The ISO shall be responsible for the analysis, selection, and appropriate use of information security tools. The ISO shall also assist the IRM staff in the establishment of security baselines and controls for networks, hosts, applications and users.

DEFINITIONS

Business Transactions: Procedures, electronic or manual, that are part of the overall mission of the business unit. This type of transaction is defined in order to distinguish it from system administration transactions.

Electronic devices: Electronically controlled devices that either store data, run programs, execute commands, or transmit information. Electronic devices include but are not limited to USB port memory sticks, laptops, personal digital assistants (PDA), and camera phones.
Remote Access: computing device access from outside the Department's private, trusted network. This access includes modem dial up, web access to applications, and direct connections with remote organizations.
Third Party: Any entity, such as state agency, department, office, division, board, bureau, commission, vendor that is not governed by the Department of Civil Service. Department of Civil Service workforce members are not third parties.
Third Party User: an individual that works for the Third Party and uses DCS computing resources and/or data.
Workforce Member: Staff, contractor, volunteer, intern working for or on behalf of the Department of Civil Service.

REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA), Security Regulation, Privacy and Security Regulation
- New York State Cyber Security Policy P03-002
- Information technology – Code of practice for information security management, ISO/IEC 17799

Policy Name	ANTI-VIRUS PROTECTION
Category	Security
Policy Number	1.09
Policy Owner	Information Security Officer (ISO)
Policy Level	Department
Effective Date	October 1, 2007
Revision Date	October 1, 2008

PURPOSE

To ensure that controls are implemented across the Department's computing resources to prevent and detect the introduction of malicious software.

POLICY STATEMENT

Information Resource Management (IRM) must implement anti-virus technical controls to detect and prevent malicious software from being introduced to the Department computing environment. IRM must consider the types of anti-virus technical controls and timeliness of updating of these controls on a routine basis, dependent on the ongoing risk assessment and the sensitivity of the information that could be potentially at risk.

Virus signature files must be updated in a timely manner, based on the ongoing risk assessment. Regular updates are required.

On network production systems or servers, the signature files will be updated in a timely manner, based on the ongoing risk assessment. In the absence of a risk assessment, either daily updates must occur, or when the anti-virus software vendor's signature files are updated and published, whichever is later.

All employees are responsible for abiding by all requirements in the *Acceptable Use Policy* to assist in the protection of the Department's computing resources and information assets in regard to protection against malicious software.

Virus outbreaks must be fully documented and reported to the security incident response team. Refer to *Security Incident Response and Management Policy*.

DEFINITIONS

Anti-Virus Software: Software that can be installed to prevent and detect the introduction of malicious software.
Malicious Software: software such as computer viruses, network worm programs and Trojan horses that can cause serious damage to networks, workstations and business data or could cause the unauthorized disclosure of sensitive information.
Virus: A program that replicates itself on computer systems by incorporating itself into other programs that are shared among computer systems. Once in the new host, a virus may damage data in the host's memory, add data on the local drive and any mapped network drive, display unwanted messages, crash the host or, in some cases, simply lie dormant until a specified event occurs.

Worm: A program similar to a virus that replicates itself over a network, consuming large quantities of network resources.

REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA), Security Regulation, Privacy and Security Regulation
- New York State Cyber Security Policy P03-002
- Information technology – Code of practice for information security management, ISO/IEC 17799

Policy Name	MONITORING SYSTEM ACCESS AND AVAILABILITY
Category	Security
Policy Number	1.10
Policy Owner	Information Security Officer (ISO)
Policy Level	Department
Effective Date	October 1, 2007
Revision Date	October 1, 2008

PURPOSE

To ensure the detection of unauthorized activities, system and application unavailability, and to provide information for capacity planning.

POLICY STATEMENT

Systems must be monitored to record and review events to detect deviation from access control policy, to detect deviation from system availability requirements, and to provide evidence in case of security incidents. Monitoring controls must be established and reviewed based on conformity to the access control policy and availability requirements.

The risk factors that are monitored are based on the criticality of the application processes, the sensitivity of the information involved, the past experience of system infiltration and misuse, and the extent of system interconnections.

The areas of risk in monitoring for system access and use and availability will change with technology changes, incident reporting, and deployment of new applications/systems.

Event logging must be designed to support all anticipated investigations of security incidents. Event log accuracy measures must be implemented. Technical or operational procedures must be developed and maintained to synchronize system clocks and to verify that system clocks do not vary significantly.

Routine log review is required. The design of log review must also be responsive to the risk factors and the risk areas. Automated alerts may be implemented.

In monitoring system access and use, the areas in scope must include, but not be limited to: user, date and time of key events, type of event, program/utilities used, use of privileged accounts, system start-up and stop, device attachment, and suspected violations of access control policy. When technically feasible, files accessed should be monitored. In monitoring system availability, the areas in scope must include, but not be limited to console alerts or messages, system log exceptions, network management alarms, and application availability.

Access to the system log(s) is restricted to designated system administrators. A list of approved system administrators must be maintained by the security office. Occasional reviews of the system log access approval list will occur without notice. All access to system logs must be logged and monitored. Additional protections must be applied to protect the system log from alteration, overwriting, or failure to record.

Disabling any type of system logging service without written authorization is prohibited, will be considered a security incident, and will be investigated.

Log files will be retained, deleted and purged according to a schedule. If an investigation has begun, the log files will not be purged for the time period of interest to the investigation.

Workforce members should be advised that monitoring of their system use is occurring. All DCS systems can be subject to user monitoring. This monitoring of system use may include the sites visited.

Division Directors must supervise system use to ensure compliance with this and other related policies. Workforce members may be required to participate in security incident investigations. All workforce members are required to report security incidents to a manager and/or the ISO.

Refer to *Access Control Policy, Acceptable Use Policy*, *Security Incident Response and Management Policy.*

DEFINITIONS

Workforce Member: Staff, contractor, volunteer, intern working for or on behalf of the Department of Civil Service.

REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA), Security Regulation, Privacy and Security Regulation
- New York State Cyber Security Policy P03-002
- Information technology – Code of practice for information security management, ISO/IEC 17799

Policy Name	USER ACCOUNTS
Category	Security
Policy Number	1.11
Policy Owner	Information Security Officer (ISO)
Policy Level	Department
Effective Date	October 1, 2007
Revision Date	October 1, 2008

PURPOSE

To prevent unauthorized access to Department computing resources and information assets.

POLICY STATEMENT

Access to computer systems must be provided through the use of individually assigned unique computer identifiers.

The Department will employ a user management process of generating, distributing, modifying, suspending, and deleting user accounts for access to resources, including privileged user accounts. Users with privileged accounts should only use these accounts to carry out administrative tasks that require privileged access; accounts with non-privileged rights should be used for routine tasks. Privileged accounts shall be monitored and misuse investigated.

The use of shared accounts must be approved by the ISO. User registration standards for external users must be defined by the Division Director/Information Owner. All third party accounts must have a termination date. Refer to *Third Party Connection and Data Exchange Policy*.

All privileged accounts must be monitored and suspected misuse of these accounts must be promptly investigated. Passwords of privileged accounts must be changed regularly.

All accounts must be reviewed periodically.

Password rules must be mandated by automated system controls whenever possible. Refer to *Acceptable Use Policy* for password best practices. Complex passwords must be enforced for remote access to the network. Refer to *Remote Access Policy* and *Third Party Connection and Data Exchange Policy*.

Information Resource Management is responsible for creating, suspending, disabling, and deleting user accounts based on instructions from Office of Human Resources Management. They are also responsible for granting access permissions to users based on instructions from the appropriate authorizing manager. Additionally, these administrators, in conjunction with Director of Internal Audit, are responsible for monitoring information system activity to identify potential security events, verifying that access permissions are being properly implemented, resetting passwords, and assisting users with difficulties involving system and network access.

DEFINITIONS

Information Asset: All categories of information, including but not limited to: records, files, and databases.
Privileged Account: The account of an individual whose job responsibilities require special system authorization, such as a network administrator, security administrator, system administrator.
Remote Access: computing device access from outside the Department's private, trusted network. This access includes modem dial up, web access to applications, and direct connections with remote organizations.
Suspending an Account: Making an account not usable while not deleting the account or account information.
Third Party: Any entity, such as state agency, department, office, division, board, bureau, commission, vendor that is not governed by the Department of Civil Service. Department of Civil Service workforce members are not third parties.
Third Party User: an individual that works for the Third Party and uses DCS computing resources and/or data.
Workforce Member: Staff, contractor, volunteer, intern working for or on behalf of the Department of Civil Service.

REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA), Security Regulation, Privacy and Security Regulation
- New York State Cyber Security Policy P03-002
- Information technology – Code of practice for information security management, ISO/IEC 17799

Policy Name	REMOTE ACCESS
Category	Security
Policy Number	1.12
Policy Owner	Information Security Officer (ISO)
Policy Level	Department
Effective Date	October 1, 2007
Revision Date	October 1, 2008

PURPOSE

To establish security controls for users accessing the Department of Civil Service's computing resources and information assets from a remote location.

POLICY STATEMENT

Remote access connections to the Department of Civil Service's network must be done in a secure manner to preserve the integrity of the network, data transmitted over that network, and the availability of the network. All remote access requests must be reviewed for appropriateness of access and to ensure that the work environment at the remote location provides adequate security. Of consideration are:

1. physical security of the remote location
2. sensitivity of the information that may be accessed and transmitted
3. current level of risk of unauthorized access to information or resources from other people using the accommodation, e.g. family and friends
4. the suitability of the communication equipment, including methods for securing remote access
5. anti-virus software and method for maintaining current signature files
6. firewalls and intrusion detection techniques at the remote location
7. encryption of personal, private or sensitive information (PPSI) in transit and on the local computer workstation
8. family and visitor access to equipment and information
9. the provision of hardware and software support and maintenance
10. the procedures for back-up
11. audit and security monitoring
12. revocation of authority, access rights and the return of equipment, if applicable, when the remote access activities cease
13. segregation of remote networks accessing the Department networks

Remote access users must have a legitimate business need and be approved by their manager, the applicable Division Director/Information Owner, and the ISO.

All remote access to the Department's network must use designated remote access gateways and authorized user accounts. Centralized and secure mechanisms for dial up must be in place. Individual accountability must be maintained at all times during remote access. Identification and authentication of the entity requesting access must be performed in such a manner as to not disclose the password or other authentication information that could be intercepted and used by a third party. Remote access points shall be monitored.

Remote users connected to the Department's network must not be simultaneously connected to any other network such as third party agency networks or separate dial-up connections to the Internet.

Under no circumstances will a user attempt to add a remote access server to the network.

The remote user must ensure the physical security of the remote location. The remote user must use best practices to protect any password(s) used when working from a remote location. The computer used for the remote access must have a firewall and up-to-date anti-virus software. All workforce members must have signed an *Acceptable Use Policy* prior to gaining approval for remote access. All third party users must have signed a *Third Party Connection and Data Exchange Agreement* prior to gaining approval for remote access. Third party remote access is also addressed in the *Third Party Connections and Data Exchange Policy*.

Division Directors shall be accountable to ensure that employees and contractors are provided with approved access to the Department network.

The ISO shall regularly determine and review the various methods of connectivity into the Department networks for the appropriateness of the controls. A risk assessment must be conducted annually.

DEFINITIONS

Remote Access: computing device access from outside the Department's private, trusted network. This access includes modem dial up, web access to applications, and direct connections with remote organizations.
Third Party: Any entity, such as state agency, department, office, division, board, bureau, commission, vendor that is not governed by the Department of Civil Service. Department of Civil Service workforce members are not third parties.
Third Party User: an individual that works for the Third Party and uses DCS computing resources and/or data.
Workforce Member: Staff, contractor, volunteer, intern working for or on behalf of the Department of Civil Service.

REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA), Security Regulation, Privacy and Security Regulation
- New York State Cyber Security Policy P03-002
- Information technology – Code of practice for information security management, ISO/IEC 17799

Policy Name	THIRD PARTY CONNECTION AND DATA EXCHANGE
Category	Security
Policy Number	1.13
Policy Owner	Information Security Officer (ISO)
Policy Level	Department
Effective Date	October 1, 2005
Revision Date	October 1, 2006

PURPOSE

To ensure that 1) a secure method of network connectivity between the Department of Civil Service and all third parties are used and to provide a formalized method for the request, approval and tracking of such connections, and 2) to ensure secure controls for information that is released outside of DCS.

POLICY STATEMENT

All Third Party connection and data exchange requests must be approved by the ISO or designee. All requests for Third Party connections and data exchanges must be submitted to the ISO by Division Directors/Information Owners. Division Directors/Information Owners may permit a Third Party to create, receive, maintain, or transmit sensitive DCS information only if the Third Party provides satisfactory assurances that the third party will appropriately safeguard the information. The satisfactory assurances must be documented in the Third Party Connection and Data Exchange Agreement and signed by the Third Party.

Division Directors/Information Owners must evaluate and document the level of sensitivity of the information to be created, received, maintained, or transmitted by the Third Party.

Information Resource Management (IRM) is responsible for the security review of the request, account creation, installation and configuration for the Third Party connection, and determination of the data exchange method.

As a part of the request and approval process, the technical and administrative contact within Third Party's organization, if authorized, or an authorized officer of the Third Party will be required to read and sign the Third Party Connection and Data Connection Agreement.

The Third Party must require that each third party user completes a Third Party Acceptable Use Policy and User Agreement. The Third Party must ensure that DCS is notified by fax or mail when the user base changes, following the specifications in the Third Party Connection and Data Exchange Agreement.

1. Right to Use Connection. Third Party may only use the connection and the information obtained from DCS for business purposes as outlined by the Third Party Connection and Data Exchange Request Requirements Document (Attachment 2*).*

2. Data Exchange.

2.1 Third Party may only use the data obtained for purposes outlined by the Third Party Connection and Data Exchange Request Requirements Document (Attachment 2) and the contract or Memoranda of Understanding, if any, that exists between DCS and Third Party for the provision of goods or services or governing conduct between DCS and Third Party with respect to the access to and use of DCS data.

2.2 Data exchange may be conducted only by methods and/or services outlined by the Third Party Connection and Data Exchange Request Requirements Document (Attachment 2). Third Party should expect that access to information and services may be limited, as determined or required by DCS.

3. Network Security.

3.1 Third Party will allow only its own employees approved in advance by DCS ("Third Party Users") to access the Network Connection or any DCS-owned equipment. Third Party shall be solely responsible for ensuring that Third Party Users are not security risks, and upon DCS' request, Third Party will provide DCS with any information reasonably necessary for DCS to evaluate security issues relating to any Third Party User.

3.2 Third Party will promptly notify DCS whenever any Third Party User leaves Third Party's employ or no longer requires access to the connection or DCS-owned Equipment.

3.3 Each Party will be solely responsible for the selection, implementation, and maintenance of security procedures and policies that are sufficient to ensure that (a) such party's use of the connection (and Third Party's use of DCS-owned Equipment) is secure and is used only for authorized purposes, and (b) such Party's business records and data are protected against improper access, use, loss alteration or destruction.

3.4 The preferred connectivity method is via the Internet to a DCS-approved or DCS-provided Virtual Private Network (VPN) device. If the device is DCS-provided, DCS will loan the Third Party, in accordance with the DCS Equipment Loan Agreement, the required client software for establishing VPN connections with DCS. Normal DCS perimeter security measures will control access to the internal network.

3.5 Extranet – Designated routers are used in combination with firewall rules to allow access to be managed. A second authentication may be required.

3.6 Remote Access - Using the DCS-provided remote access software, Third Party will connect via an Internet browser. The account may be disabled until usage is required and controls are placed and managed by DCS. Third Party will be required to follow procedures to enable the account for each use.

3.7 Third Party Connections will be audited. All remote access user accounts for Third Parties will be given an expiration time. Renewals must be requested by

Third Party and approved by the Department Sponsor. Obsolete Third Party connections will be terminated.

3.8 Software versions on all Third Party computers that connect to the DCS network must be versions that are currently supported by the software manufacturer, and all available security updates and hot fixes for that software must be applied in a timely fashion. Software and firmware for all Third Party networking equipment that is part of the connection to the DCS network must be kept up to date, especially with patches that fix security vulnerabilities.

3.9 Anti-virus software and firewalls must be installed and enabled at all times on DCS-owned computers and on Third Party computers that connect to the DCS network. Additionally, virus definition files must be kept up to date.

3.10 In no case may a Third Party Connection to DCS be used as an Internet Connection for Third Party or for a Third Party User.

4. Notifications.

4.1 Third Party shall notify DCS in writing promptly of any change in its Users for the work performed over the Network Connection or whenever Third Party believes a change in the connection and/or functional requirements of the connection is necessary.

Any notices required by this Agreement shall be given in hand, sent by first class mail, or via facsimile to the applicable address set forth below.

Third Party:	NYS Department of Civil Service:
_____	State Campus, Building One
_____	Albany, New York 12239
_____	
Attention: _____	Attention: _____
_____	_____

5. Citizen Notification

If Third Party maintains "identifying personal information" on behalf of the Department and such information is compromised, Third Party shall notify the Department immediately that the information has been compromised, the circumstances under which the information was compromised, and the measures undertaken by Third Party to address those circumstances and to otherwise mitigate the effects of the compromise. If encrypted data is compromised along with the corresponding encryption key and encryption software, the data shall be considered unencrypted and the information will be considered compromised through unauthorized access. If the Department requests Third Party to do so, Third Party shall notify the persons whose identifying information was compromised. Such notification shall be communicated via postal service or email, as directed by the Department, and shall otherwise be executed in accordance with the Department's direction. Notification shall be delayed if a law enforcement agency determines that such notification may impede a criminal investigation. For the purpose of this section, "identifying personal information" shall be any information concerning an individual which, because of name, number, symbol, mark or other identifier in combination with any of the following, is unencrypted: (1) Social Security Number; or

(2) driver's license number; or (3) financial account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account; or (4) password which would permit access to the individual's account.

6. Payment of Costs. Each Party will be responsible for all costs incurred by that Party under this Agreement, including, without limitation, costs for phone charges, telecommunications equipment and personnel for maintaining the connection.

7. Confidentiality.

7.1 Information exchanged for the business purposes outlined in Attachment 2 will be held confidential by the Parties to the maximum extent permitted by law. Each Party may internally use the information received from the other Party hereunder in connection with and as specifically necessary to accomplish the Business Purpose set forth in Attachment 2 and for no other purposes. Each Party may otherwise share such information with other third parties (e.g. consultants, subcontractors, control agencies) as required or permitted by law in order to effect the business purposes outlined in Attachment 2 and for no other purposes, provided that such third parties agree to the confidentiality restrictions set forth herein and as may be required otherwise by State and federal law.

7.2 Third Party must implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the sensitive information that it creates, receives, maintains, or transmits on behalf of DCS.

7.3 Unencrypted DCS information must not be transmitted over email.

7.4 Third Party must ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it and report to the DCS Help Desk any security incident of which it becomes aware.

8. Third Party Users

8.1 Third Party must require that each Third Party User executes a Third Party Acceptable Use Policy and Agreement (Attachment 3). Third Party must ensure that DCS is notified by fax or mail when the user base changes, following the specifications in the Third Party Connection & Data Exchange Agreement.

8.2 All aspects of Third Party connections within DCS control may be monitored by the appropriate DCS support group and/or the DCS ISO. Any unauthorized use or change to devices will be investigated immediately.

8.3 All Third Party Connections will be reviewed on a regular basis and information regarding specific Third Party connection will be updated as necessary. Obsolete Third Party connections will be terminated.

9. DCS-owned Equipment.

9.1 DCS may, in DCS' sole discretion, loan to Third Party certain equipment and/or software for use on Third Party premises (the DCS-owned Equipment) under the terms of the DCS Equipment Loan Agreement set forth in Attachment 4. DCS-owned equipment will only be configured for TCP/IP, and will be used solely by Third Party on Third Party's premises or other locations authorized by DCS for the purposes set forth in this Agreement. DCS is responsible for ensuring that it has the right under applicable software licenses to permit third party use.

9.2 Third Party may modify the configuration of the DCS-owned equipment only after notification and approval in writing by authorized DCS personnel.

9.3 Third Party will not change or delete any passwords set on DCS-owned equipment without prior approval by authorized DCS personnel. Promptly upon any such change, Third Party shall provide DCS with such changed password.

DEFINITIONS

Department Sponsor: An individual in the DCS business unit that acts as custodian and requester for the third party connection. Often this is the Information Owner/Division Director or the Data Custodian.

Remote Access: computing device access from outside the Department's private, trusted network. This access includes modem dial up, web access to applications, and direct connections with remote organizations.

Third Party: Any entity, such as state agency, department, office, division, board, bureau, commission, vendor that is not governed by the Department of Civil Service. Department of Civil Service workforce members are not third parties.

Third Party User: an individual that works for the Third Party and uses DCS computing resources and/or data.

Workforce Member: Staff, contractor, volunteer, intern working for or on behalf of the Department of Civil Service.

REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA), Security Regulation, Privacy and Security Regulation
- New York State Cyber Security Policy P03-002
- Information technology – Code of practice for information security management, ISO/IEC 17799

Policy Name	INFORMATION SYSTEM DEVELOPMENT
Category	Security
Policy Number	1.14
Policy Owner	Information Security Officer (ISO)
Policy Level	Department
Effective Date	October 1, 2007
Revision Date	October 1, 2008

PURPOSE

To ensure that security is built into information systems, and to prevent loss, modification or misuse of user data in information systems in production.

POLICY STATEMENT

To ensure that security is built into information systems, statements of business requirements for new information systems, or enhancements to existing information systems. Specifications must address security needs and include requirements for controls. Such specifications must consider the automated controls to be incorporated in the system, and the need for supporting manual controls. Similar considerations must be applied when evaluating software packages for business applications. The ISO must be involved in all phases of the lifecycle of system development, from the requirements definition phase through implementation and eventual application retirement.

Security requirements should reflect the sensitivity of the information assets. The framework used to identify controls is the risk assessment and risk management framework. Refer to *Data Classification Policy* and *Risk Analysis and Management Policy*. Procedural, technical and administrative controls should address:

1. Audit controls
2. Data input validation
3. Internal processing controls
4. Message integrity
5. Output data validation
6. The possible need for cryptographic controls
7. Security of system files

All specific control mechanisms must be documented.

Test Data

Once test data is developed, it must be protected and controlled for the life of the testing to ensure a valid and controlled simulation with predictable outcomes.

Production data may be used for testing only if all of the following controls are applied;

1. A business case is documented and approved in writing by the Division Director/Information Owner and access controls, system configurations and logging requirements for the production data are applied to the test environment; or

2. A business case is documented and approved in writing by the Division Director/Information Owner and Personal, Private or Sensitive Information (PPSI) will be masked or overwritten with fictional information and the data will be deleted as soon as the testing is completed.

Change Control Processes
To minimize the possibility of corruption of information systems, formal change control procedures for business applications must be developed, implemented and enforced. The procedures must ensure that security and control procedures are not compromised, that support programmers are given access only to those parts of a system necessary to perform their jobs, and that formal agreement and approval processes for changes are implemented. These change control procedures will apply to business applications as well as systems software used to maintain operating systems, network software, and hardware changes.

Source Code Libraries
In addition, access to source code libraries for both business applications and operating systems must be tightly controlled to ensure that only authorized individuals have access to these libraries and that access is logged to ensure all activity can be monitored.

Restrictions on Changes to Software Packages
Modifications to software packages are discouraged. Where it is deemed essential to modify a software package, the following points must be addressed:

1. The risk of built-in controls and integrity processes being compromised
2. Whether the consent of the vendor should be obtained
3. The possibility of obtaining the required changes from the vendor as standard program updates
4. The impact if the organization becomes responsible for the future maintenance of the software as a result of changes

Outsourced Software Development
Where software development is outsourced, the following points should be considered:

1. Licensing arrangement, code ownership and intellectual property rights
2. Certification of the quality and accuracy of the work carried out
3. Escrow arrangements in the event of failure of the third party
4. Rights of access for audit of the quality and accuracy of work done
5. Contractual requirements for quality of code
6. Testing before installation to detect Trojan code

DEFINITIONS

Information System: 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.

REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA), Security Regulation, Privacy and Security Regulation
- New York State Cyber Security Policy P03-002
- Information technology – Code of practice for information security management, ISO/IEC 17799

Policy Name	SECURITY INCIDENT RESPONSE AND MANAGEMENT
Category	Security
Policy Number	1.15
Policy Owner	Information Security Officer (ISO)
Policy Level	Department
Effective Date	October 1, 2007
Revision Date	October 1, 2008

PURPOSE

To minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents.

POLICY STATEMENT

All workforce members must work to contribute to an effective Department incident response and management process that results in a prompt and organized response to security incidents.

Each workforce member must understand his/her role and responsibilities regarding information security issues and protecting the Department's information. Workforce members are required to report any observed or suspected incidents to a manager and/or the ISO or security designee immediately. Workforce members must not attempt to prove a suspected weakness or incident.

Examples of suspected security incidents are:

1. Unsecured protected computing resources
2. Any unsupervised or otherwise unauthorized person in a server area or a protected area
3. Release of internal directories or other documentation that provides locations of server areas
4. Attempts by an unauthorized individual to obtain access credentials, e.g., ID badges, security access codes, keys.
5. Unauthorized attempts to gain access to DCS network systems or facilities
6. Unapproved hardware connected to the DCS network
7. Hardware left in an unsecured area
8. A potential fire or water hazard
9. Damaged equipment, facilities or utilities
10. Loss or misplacement of media (e.g. disks, tapes, paper) containing Personal, Private, or Sensitive Information (PPSI)
11. Inappropriate use of the computing environment
12. Disclosure of PPSI
13. Other violations to the *Acceptable Use Policy*

Managers receiving a security report must report the incident upward to the ISO. It is the ISO's responsibility to establish an incident investigation and alert Information Resource Management (IRM) and affected Divisions of possible damages. IRM, including the Help Desk, and affected Divisions receiving an alert must act immediately, or as described on the ISO alert.

The ISO must notify the Information Security Team of all reported incidents. The Information Security Team must document the symptoms of the problem and must take steps to isolate the problem immediately. The Information Security Team and other workforce members will be identified to assist with analysis and identification of the cause of the incident, planning and implementation of corrective actions to prevent reoccurrence, collection of audit log information, and communication with those affected by or involved in the recovery from the incident.

To capture recurring incidents and to record lessons learned, the Information Security Team must ensure that all incidents are tracked by type and that information on volumes of security incidents and malfunctions is gathered.

Because the act of testing weaknesses could have unintended consequences, workforce members must not attempt to prove a suspected weakness unless specifically authorized by the ISO to do so.

Disciplinary action, consistent with the Civil Service Law and the negotiated agreements, will be brought against any employee of the Department found to be engaging in such incidents or who retaliates against any employee who reports or complains of activities related to an incident.

Feedback on investigations must be provided regularly and promptly to the ISO. Individuals reporting incidents will be notified when the incident has been closed. The details of the incident review, including the resolution, are confidential and will not be disclosed to the reporting individual.

The Office of Cyber Security Critical Infrastructure and Coordination will receive incident reports from the ISO. The ISO is responsible for all external reporting and notification.

See also Policy 1.24, *Citizen Notification*, for special procedures relating to security breaches that may have disclosed the private information of any New York State residents to unauthorized persons.

DEFINITIONS

Information Security Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Workforce Member: Staff, contractor, volunteer, intern working for or on behalf of the Department of Civil Service.

REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA), Security Regulation, Privacy and Security Regulation
- New York State Cyber Security Policy P03-002
- Information technology – Code of practice for information security management, ISO/IEC 17799

Policy Name	CONTINGENCY PLANNING
Category	Security
Policy Number	1.16
Policy Owner	Information Security Officer (ISO)
Policy Level	Department
Effective Date	October 1, 2007
Revision Date	October 1, 2008

PURPOSE

To ensure the continuity of critical operations, the protection of information assets, and the prevention of damage to computing resources in the event of an emergency, disaster, or other occurrence that damages or compromises computing resources, information assets, or business functions.

POLICY STATEMENT

The Department of Civil Service requires each Division to participate in a Department-wide contingency planning effort to establish and implement policies and procedures for responding to an emergency or other occurrence that damages or compromises computing resources, information assets, and business functions. In addition, the Department is committed to compliance with Federal and State regulations including the Health Insurance Portability Accountability Act (HIPAA) Security rule that requires contingency planning for responding to an emergency or other occurrence that damages or compromises systems that contain electronic protected health information. Division contingency planning efforts must result in written plans. These plans may include a Contingency Plan, a Disaster Recovery Plan and a Business Continuity Plan. Plans must be maintained to a current state of readiness.

Contingency plans must be developed and must be written in coordination between other emergency preparedness planning efforts including, but not limited to, emergency preparedness planning and crisis communication planning. Contingency plans must be written with input and support from other planning efforts such as cyber-incident response planning, monitoring planning, and auditing planning. Contingency plans must be developed in relation to sensitivity levels assigned by Division Directors/Information Owners to each information asset. Contingency plans must be compatible with program requirements for the business and support functions.

The scope of the contingency planning must include:

- Organizational framework for contingency efforts including the roles and responsibilities of team members.
- Scope as applied to the type of platform and organizational functions subject to the planning
- Procedures for responding to an emergency or other occurrence that damages or compromises computing resources and/or information assets in the Department.
- List of applications with Private, Personal or Sensitive Information (PPSI) including those with protected health information.

- Procedures for system/application backup planning, including frequency of backups and storage of backup media.
- Procedures for system/application recovery.
- Procedures for the continuity of system support.
- Enabling the continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.
- Coordination with system development projects to ensure that contingency is addressed in each system development lifecycle phase.
- Business recovery goals and procedures, by priority, based on a business impact analysis.
- Notification, plan activation, and plan deactivation procedures.
- Resource requirements, training requirements, exercise and testing schedules.
- Plan maintenance schedule.
- Maintenance and distribution responsibilities.

DEFINITIONS

Information Asset: All categories of information, including but not limited to: records, files, and databases.
Information Owner: The Division Director that has responsibility for making classification and control decisions regarding use of information assets.
Workforce Member: Staff, contractor, volunteer, intern working for or on behalf of the Department of Civil Service.

REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA), Security Regulation, Privacy and Security Regulation
- New York State Cyber Security Policy P03-002
- Information technology – Code of practice for information security management, ISO/IEC 17799
- National Institute of Standards and Technology (NIST), Contingency Planning Guide for Information Technology Systems, SP 800-34

Policy Name	SYSTEM BACKUP AND RESTORATION
Category	Security
Policy Number	1.17
Policy Owner	Information Security Officer (ISO)
Policy Level	Department
Effective Date	October 1, 2007
Revision Date	October 1, 2008

PURPOSE

To ensure that interruptions to normal business operations are minimized and that sensitive business applications and processes are protected from the effects of major failures.

POLICY STATEMENT

To ensure that interruptions to normal business operations are minimized and that sensitive business applications and processes are protected from the effects of major failures, a comprehensive backup strategy must be developed and maintained, based on a risk assessment and the sensitivity of each information asset. The Division Director/Information Owner, in cooperation with the Information Security Team and Information Resource Management (IRM), must ensure that regular backups are created of all sensitive information that is stored on network file servers or production servers. IRM must develop plans that can meet the backup and recovery requirements of the Division. Retention requirements must be determined by the Division Director/Information Owner. If personal, private or sensitive information (PPSI) is stored on a personal computer, the owner of that data is responsible for backing up that information. All users must follow the instructions of Division Directors/Information Owners on the proper storage and disposal of electronic information.

Routine backups of the operating system, programs, applications, and data files must be performed. Backup tapes and removable media must be stored in a secure facility offsite. A separate network should be used for backups where feasible. Access to the back-up network must be restricted. Back-up equipment, tape library and tapes must be kept in a secure area. Only authorized workforce members will be allowed to enter this secured area. Personnel charged with performing backups will receive training. The backup planning efforts should keep training requirements in mind. Backup and recovery procedures must be fully documented and must be tested regularly. Backup procedures must include procedures to be followed whenever equipment is moved. Requests for data restores must be authorized by the Data Custodian for that information asset.

The ISO and the Information Security Team must review the physical and logical security controls used in the backup strategy and recommend changes to the process when information security considerations warrant the changes.

Refer to *Data Classification Policy*.

DEFINITIONS

Data Custodian: The individual appointed by the Division Director/Information Owner to make decisions on their behalf.
Information Asset: All categories of information, including but not limited to: records, files, and databases.
Information Owner: The Division Director that has responsibility for making classification and control decisions regarding use of information assets.
Sensitivity: The measurable, harmful impact resulting from disclosure, modification, or destruction of information. There are three measures of sensitivity for every information asset: confidentiality, integrity, and availability.
Workforce Member: Staff, contractor, volunteer, intern working for or on behalf of the Department of Civil Service.

REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA), Security Regulation, Privacy and Security Regulation
- New York State Cyber Security Policy P03-002
- Information technology – Code of practice for information security management, ISO/IEC 17799

Policy Name	AUDIT AND COMPLIANCE
Category	Security
Policy Number	1.18
Policy Owner	Information Security Officer (ISO)
Policy Level	Department
Effective Date	October 1, 2007
Revision Date	October 1, 2008

PURPOSE

To avoid breaches of any criminal and civil law, statute, regulation or contract; to ensure compliance of systems with organizational security policies and standards; and to maximize the effectiveness of and to minimize interference to/from the system audit process.

POLICY STATEMENT

An effective ongoing audit process is an important component of the Department security and risk management program. The Department is subject to both external and internal audits on a regular basis and as deemed necessary by the Director of Internal Audit. At a minimum, the Director of Internal Audit conducts a comprehensive annual review of the Department's computer network policies and procedures.

The Director of Internal Audit performs independent checks of the Information Security Team, using audit software to track administrative activities for unauthorized access and sign-on attempts. Additionally, in the course of normal system maintenance and administration, the Information Security Team must periodically test the effectiveness of the controls of its own logical and administrative security control systems.

On at least an annual basis and whenever operational or environmental changes affect the security of sensitive information, the Department, through the direction of the ISO, shall review security policies and procedures to ensure that they continue to meet all legal and regulatory requirements and relevant best practices.

Regular reporting on the effectiveness of compliance efforts shall be accomplished by the ISO. The Department shall have the expectation of CSCIC reviews. The Department will evaluate compliance against the CSCIC policy annually and develop appropriate mitigation plans.

All workforce members are responsible for ensuring that all relevant security processes and procedures are followed and can expect regular reviews of compliance. Workforce members shall report any compromise or suspected compromise to management. Refer to *Security Incident Response and Management Policy*.

The Director of Internal Audit is responsible for regularly auditing information security controls and practices to ensure compliance with all relevant Department security policies and procedures.

The ISO or his/her designee is responsible for overseeing regular reviews of information system activities to verify compliance with security policies and to be aware the risks to which

information assets are vulnerable. Additionally the ISO or his/her designee is responsible for evaluating the extent to which the information security program and its policies are still in compliance with relevant laws and regulations. The Office of the Counsel will assist the ISO in this effort.

DEFINITIONS

Information Asset: All categories of information, including but not limited to: records, files, and databases.

Workforce Member: Staff, contractor, volunteer, intern working for or on behalf of the Department of Civil Service.

REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA), Security Regulation, Privacy and Security Regulation
- New York State Cyber Security Policy P03-002
- Information technology – Code of practice for information security management, ISO/IEC 17799

Policy Name	POLICY REVIEW AND REVISION
Category	Security
Policy Number	1.19
Policy Owner	Information Security Officer (ISO)
Policy Level	Department
Effective Date	October 1, 2007
Revision Date	October 1, 2008

PURPOSE

To establish a process for revising the Department's Information Security Policy.

POLICY STATEMENT

Policy revisions may be required as the business needs of the Department change, as the technology environment advances, as additional compliance issues arise, and when business environment changes demand a more robust security orientation. In addition, all information security policies must have a scheduled review date and must be reviewed at that time for revisions. When making the decision to revise these policies, the following should be considered:

- Whether or not there is an acceptable alternative to the established policy
- When a particular business function cannot be performed effectively if the policy is not revised
- When a business function is no longer cost-effective by following the policy as written
- When failure to change the policy would result in an unacceptable level of risk to the Department

Requests for policy changes can be sent to the ISO, briefly stating the underlying business problem and recommended approach. The ISO will be responsible for maintaining overall Information Security Policies. Should any exceptions to these policies be granted, they will be documented and maintained by the ISO.

The Information Security Steering Committee is chaired by the ISO, and includes representatives from Information Resource Management, Office of Human Resources Management, the Office of Financial Administration, Director of Internal Audit, and the Office of the Counsel. The Information Security Steering Committee oversees the activities and deliverables of the Information Security Team and formulates Department of Civil Service information security policy and strategy. The Commissioner's Office has final approval authority over all policies, protocols, standards, guidelines, and procedures.

Exceptions to this policy must be first submitted for approval to the Division Director/Information Owner and then to the ISO. The ISO will be responsible for maintaining this policy and obtaining approval for changes.

DEFINITIONS

Information Owner: The Division Director that has responsibility for making classification and control decisions regarding use of information assets.

REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA), Security Regulation, Privacy and Security Regulation
- New York State Cyber Security Policy P03-002
- Information technology – Code of practice for information security management, ISO/IEC 17799

Policy Name	RISK ASSESSMENT AND MANAGEMENT
Category	Security
Policy Number	1.20
Policy Owner	Information Security Officer (ISO)
Policy Level	Department
Effective Date	October 1, 2007
Revision Date	October 1, 2008

PURPOSE

To enable the Department to identify risks to the confidentiality, integrity, and availability of the Department's information assets and computing resources, and to determine reasonable and appropriate security measures to address those identified risks.

POLICY STATEMENT

The Department must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the Department's information assets and computing resources, and then determine and implement security measures sufficient to reduce the risks and vulnerabilities to a reasonable and appropriate level. The scope of the risk assessment should be comprehensive enough to enable these measures to be developed.

The risk assessment and management framework includes:

1. **Risk Assessment:** comprehensive annual review, measurement, and rating of security vulnerability and threats.
2. **Mitigation Strategy Development:** ongoing process of developing and refining a strategy towards resolving and addressing security risks.
3. **Intervention and Mitigation:** execution of the interventions established in the mitigation strategy
4. **Workforce Communication and Training:** utilizing communication and training techniques to explain risk mitigation efforts and to enlist partnership and participation in security risk mitigation
5. **Evaluation and Revision:** determination of success measures and revision of the mitigation strategy

Security domains that must be addressed in the risk assessment and management process include:

1. Security Policy
2. Organizational Security
3. Asset Classification and Control
4. Personnel Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. Systems Development and Maintenance
9. Business Continuity Management
10. Compliance

The ISO has the responsibility for:

- Overseeing the risk assessment and management process for the Department
- Approving the risk assessment and management strategy
- Endorsing and promoting the risk assessment and management strategy

Each Division Director/Information Owner has the responsibility for:

- Oversight of the risk management program for the Division
- Coordinating risk management activities across the Division
- Assigning of assessment team participants
- Endorsing and promoting the risk assessment processes in the Division
- Approving the risk management processes in their Division

The Information Security Team has the responsibility for:

- Developing and recommending risk management strategies and processes
- Establishing risk assessment schedules and scope
- Conducting risk assessments processes

Each Application Owner has the responsibility for:

- Participating in risk assessment interviews
- Completing risk assessment questionnaires
- Identifying and clarifying security risks
- Assigning assessment team participants

All workforce members have responsibilities to follow the security policies that DCS has established.

To reduce the security risks of new technology and workforce practices, focused security risk assessments must occur as an integral part of the introduction and design of new technologies and workforce procedures. These risk assessments are in addition to the ongoing requirement of risk assessment.

Use of vulnerability scanning and penetration testing methods to assist with risk assessment will be based on an evaluation of the environment and the development of a strategy for the use of the findings. All scanning and penetration testing requires prior approval from the ISO. Workforce members must not attempt to test vulnerabilities.

DEFINITIONS

Information Asset: All categories of information, including but not limited to: records, files, and databases.
Information Owner: The Division Director that has responsibility for making classification and control decisions regarding use of information assets.
Workforce Member: Staff, contractor, volunteer, intern working for or on behalf of the Department of Civil Service.

REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA), Security Regulation, Privacy and Security Regulation
- New York State Cyber Security Policy P03-002
- Information technology – Code of practice for information security management, ISO/IEC 17799

Policy Name	MEDIA HANDLING AND DISPOSAL
Category	Security
Policy Number	1.21
Policy Owner	Information Security Officer (ISO)
Policy Level	Department
Effective Date	October 1, 2007
Revision Date	October 1, 2008

PURPOSE

To prevent disclosure of personal, private or sensitive information (PPSI) and to prevent loss, damage, or compromise of assets and interruption to business activities.

POLICY STATEMENT

All procedures for the handling of computer and server equipment and storage media must be approved by the ISO. Computer and server handling for reassignment, service, or for disposal procedures can only be conducted by authorized Information Resource Management (IRM) individuals. IRM must ensure that hard disk drives are physically destroyed or securely overwritten when no longer to be used. IRM must ensure that PPSI is removed from computers when the computers will be reused or reassigned. Logs must be maintained for all computer and server moves.

Workforce members observed using or moving equipment or other media that is not assigned to their individual use must be reported to the manager immediately.

Workforce members must not dispose of removable media in the trash. Collection boxes for removable media must be provided in each Division and must be secured until pickup. These collection boxes must be clearly marked as security scrap and must be separate from paper security scrap. For pickup, Divisions should tape the box closed and contact Shipping.

Division Director approval must be obtained to use removable media with Department computing resources. All portable or removable media must be encrypted. Encryption keys must not be stored with portable device. Workforce members authorized to use removable media must not leave removable media unsecured on their desktops. Before removing media from the physical site, workforce members must inform their supervisor. On returning media to the physical site, workforce members must scan the media for viruses. Assistance is provided by the Help Desk.

Paper documents and printed output with sensitive information must be disposed of by either shredding the document or using the security scrap boxes supplied to each Division. Security scrap boxes must be stored in supervised areas or locked in rooms during unsupervised hours. They should not be stored within public or commonly used walkways.

When Division policies are more stringent, the Division policy will supersede this policy.

Refer to *Acceptable Use Policy* and *Physical Security Policy*.

DEFINITIONS

Removable media: storage platforms that can be separated easily from the computing resource. Examples include: removable disks of any kind, magnetic tapes, cassettes, CDs, personal digital assistants, film, memory sticks.

Workforce Member: Staff, contractor, volunteer, intern working for or on behalf of the Department of Civil Service.

REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA), Security Regulation, Privacy and Security Regulation
- New York State Cyber Security Policy P03-002
- Information technology – Code of practice for information security management, ISO/IEC 17799

Policy Name	OPERATIONAL MANAGEMENT
Category	Security
Policy Number	1.22
Policy Owner	Information Security Officer (ISO)
Policy Level	Department
Effective Date	October 1, 2007
Revision Date	October 1, 2008

PURPOSE
To ensure the correct and secure operation of information processing facilities.

POLICY STATEMENT
All Department information processing facilities must develop and maintain documented operating instructions and management processes for information security incidents. Computing hardware, software or system configurations provided by the Department must not be altered or added to in any way unless exempted by documented written policy or specific approval.

Operational and management responsibilities must be clearly defined for service provisioning by or for the Department. The Division Directors shall implement organizational structures and request system designs that segregate the activities requiring collusion to commit fraud.

Where practical, management and execution duties must be separated. Where separation is difficult to achieve, compensating controls must be implemented. The ISO and the Information Security Team shall not audit itself.

Separation of Development, Test, and Production Environments
Separation must be implemented between development and test functions. A stable quality assurance environment where testing can be conducted and changes cannot be made to the programs being tested must be ensured. Processes must be documented and implemented to govern the transfer of software between environments. The following controls must be used:

1. Development software and tools must be maintained on computer systems isolated from the production environment, either physically separate machines or separated by access controlled domains or directories.
2. Access to compilers, editors and other system utilities must be removed from production systems when not required.
3. Logon procedures and environmental identification must be sufficiently unique for production, testing and development.
4. Controls must be in place to issue short-term access to development staff to correct problems with production systems allowing only necessary access.

System Planning and Acceptance
Advance planning and preparation must be performed to ensure the availability of adequate capacity and resources. The security requirements of new information systems must be established, documented and tested prior to their acceptance and use.

Acceptance criteria must be developed and documented for new information systems, upgrades and new versions of existing systems. Testing to ensure that the security requirements are met must be performed prior to the information system being migrated to the production environment.

Covert Channels and Trojan Code
Where covert channels or Trojan code are a concern, the following must be considered:

1. Buying programs only from a reputable source
2. Buying programs in source code so the code may be verified
3. Using evaluated products
4. Inspecting all source code before operational use
5. Controlling access to, and modification of, code once installed
6. Use staff of proven trust to work on key systems

Software Maintenance
Vendor supplied software must be maintained at a level supported by the vendor. Exceptions require a waiver from the ISO. Maintenance of DCS-developed software will be logged to ensure changes are authorized, tested and accepted by DCS management. All known security patches must be reviewed, evaluated and appropriately applied in a timely manner.

Technical Review of Operating System Changes
All operating system changes must undergo both testing and a technical review. These processes should cover:

1. Review of application control and integrity procedures to ensure that they have not been compromised by the operating system changes
2. Ensuring that annual support planning will cover reviews and system testing resulting from operating system changes
3. Ensuring that notification of operating system changes is provided in time to allow appropriate reviews to take place before implementation
4. Ensuring that appropriate changes are made to the business continuity plans

DEFINITIONS

Trojan Code: Covertly-placed code that when executed performs an unauthorized activity or function. It may be activated by changing a parameter accessible by both secure and insecure elements of a computing system, or by embedding information into a data stream.

REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA), Security Regulation, Privacy and Security Regulation
- New York State Cyber Security Policy P03-002
- Information technology – Code of practice for information security management, ISO/IEC 17799

Policy Name	THIRD PARTY ACCEPTABLE USE POLICY AND AGREEMENT
Category	Security
Policy Number	1.23
Policy Owner	Information Security Officer (ISO)
Policy Level	Department
Effective Date	October 1, 2007
Revision Date	October 1, 2008

PURPOSE

To establish the Third Party Acceptable Use Policy and Agreement as a requirement for individual third party users to sign before providing access to DCS systems and data is provided.

POLICY STATEMENT

This policy and agreement applies to all forms of computer and networking use, including local access at the Department of Civil Service (DCS) premises, remote access via public or private networks, access using DCS equipment, access using individual or group accounts, and access via other methods.

A signed paper copy of this form must be submitted by any individual (1) for whom authorization of a new user account is requested, (2) who will use a shared third party account, and/or (3) who is requesting reauthorization of an existing use. Modifications to the terms and conditions of this agreement will not be accepted by DCS management.

Indicate here if this is a notification that the user no longer requires access: ☐

User's Name (print): _____

Organization: _____

Telephone Number: _____
Area code Number Extension

Office Address: _____
Street Address

Office Address (cont): _____
City State Zip

By signing this agreement, the undersigned acknowledges that he or she has read, understands, and agrees to comply with the above principles governing the use of DCS computing resources.

User Signature: _____ Date: _____

You must sign this signature page and send it to DCS. Retain a copy of the signature page and the attached Policy for your records. This form must be delivered either by fax or mail to:

Mail: NYS Department of Civil Service, Alfred E Smith Office Building, 80 Swan Street, Albany, NY 12239
Attention: Help Desk
FAX: 518-485-5588

Protection of DCS Information

All records and information maintained in DCS systems accessed by the User are confidential and shall be used by the User solely for the purpose of carrying out the User's official duties. Users may not use any such records and information for any other purpose. No such records or information may otherwise be used or released to any person by the User or by the User's employer or agent, except as may be required by applicable State or federal law or by a court of competent jurisdiction. All accounts and connections will be regularly reviewed.

Banners

All users will follow the guidelines of the DCS Log-on Banner as stated below.

> NOTICE * The contents of this banner have been recommended to all State agencies by the Office for Technology in the NYS Preferred Standards and Procedures for Information Security. * This electronic system, which includes hardware, software and network components and all data contained therein (the "system"), is the property of the New York State Department of Civil Service (DCS). * Unauthorized use or attempted unauthorized use of this system is not permitted and may constitute a federal or state crime. Such use may subject you to appropriate disciplinary and/or criminal action. Use of this system is only permitted to the extent authorized by DCS. * Use is limited to conducting official business of DCS. Under the Electronic Communications Privacy Act of 1986 (18 U.S.C. 2510, et seq.), notice is hereby given that there are NO facilities provided by this system for sending or receiving private confidential electronic communication. Any use, whether authorized or not, may be monitored, intercepted, recorded, read, copied, accessed or captured in any manner, and used or disclosed in any manner, by authorized DCS personnel without additional prior notice to users. In this regard, users have no legitimate expectation of privacy during any use of this system or in any data on this system. * Use, whether authorized or unauthorized, constitutes expressed consent for DCS to monitor, intercept, record, read, copy, access or capture and use or disclose such information. * DCS policy regarding this matter can be reviewed on the DCS internal website. Copies can also be obtained from the Office of Human Resources Management. Such policies are subject to revision. This notice is consistent with the Acceptable Use Policy issued to DCS employees regarding acceptable use, June 15, 2005. I have read and understand this notification and department policy.

Passwords

The User is not permitted to share his/her password with anyone. Passwords must never be written down. The User must not use the same password for multiple applications. The User must use passwords that are not easily guessed and must not use their email address as their password.

Shared Accounts

All use of shared accounts must be authorized by DCS. Users of shared accounts must be identified to DCS via the completion and signing of this policy/agreement. Third Parties are

responsible for notification to DCS when the user base changes. Passwords for shared accounts must not be provided to individuals who have not been identified by Third Party to DCS and who have not completed and signed this policy/agreement.

Virus Protection

Anti-virus software must be installed and enabled at all times on DCS-owned computers and on third party computers used to conduct DCS business. Virus definition files must be kept up to date. DCS Information Resource Management (IRM) provides anti-virus software and maintains the configuration of that software for all DCS-owned computers.

Acceptable Use

DCS computers, computing systems and their associated communication systems are provided to support the official business of DCS. All uses inconsistent with DCS' business activities and administrative objectives are considered to be inappropriate use.

Examples of unacceptable behavior include, but are not limited to the following.

- Any illegal activities that could result in legal actions against and/or financial damage to DCS.
- Computer usage that reasonably harasses or offends other employees, users, or outsiders, or results in public embarrassment to DCS.
- Computer usage that is not specifically approved and which consumes significant amounts of computer resources not commensurate with its benefit to DCS' mission or which interferes with the performance of a worker's assigned job responsibilities.
- Use in connection with compensated outside work or unauthorized not-for-profit business activities.
- Use of sniffers, spyware, adware or other related technology.

Software Protection

The User is responsible for complying with copyright, licensing, trademark protection, and fair use restrictions.

Reporting Incidents

Users are required to report incidents of system errors, data discrepancies, application performance problems, to the DCS Help Desk, at (518) 457-5406 phone; 518-485-5588 Fax.

DCS Rights

Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510 et seq), notice is hereby given that there are no facilities provided by this system for sending or receiving private or confidential electronic communications. DCS has access to all access attempts, messages created and received, and information created or stored using DCS resources, and will monitor use as necessary to assure efficient performance and appropriate use. Information relating to or in support of illegal activities will be reported to the appropriate authorities.

DCS reserves the right to log and monitor use. DCS reserves the right to remove a user account from the network. DCS assumes no responsibility or liability for files or information deleted.

The DCS will not be responsible for any damages. This includes the loss of data resulting from delays, non-deliveries, or service interruptions caused by negligence, errors or omissions, or caused by the way the user chooses to use DCS computing facilities.

DCS reserves the right to change its policies and rules at any time.

Penalties

The User shall hold the State and DCS harmless from any loss or damage to the State and/or DCS resulting from the User's inappropriate disclosure of information covered by this User Agreement. Further, the User's non-compliance with this Agreement may result in the revocation of system privileges, termination of employment or contract with DCS, and/or criminal and/or civil penalties.

DEFINITIONS

Remote Access: computing device access from outside the Department's private, trusted network. This access includes modem dial up, web access to applications, and direct connections with remote organizations.

Third Party: Any entity, such as state agency, department, office, division, board, bureau, commission, vendor that is not governed by the Department of Civil Service. Department of Civil Service workforce members are not third parties.

Third Party User: an individual that works for the Third Party and uses DCS computing resources and/or data.

REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA), Security Regulation, Privacy and Security Regulation
- New York State Cyber Security Policy P03-002
- Information technology – Code of practice for information security management, ISO/IEC 17799

Policy Name	CITIZEN NOTIFICATION
Category	Security
Policy Number	1.24
Policy Owner	Information Security Officer (ISO)
Policy Level	Department
Effective Date	October 1, 2007
Revision Date	October 1, 2008

PURPOSE

To establish citizen notification requirements and procedures in the case of a compromise of identifying personal information.

POLICY STATEMENT

Discovery and reporting of security breach. The Department values the protection of Personal, Private, Sensitive Information (PPSI) and takes considerable measures to secure it. Whenever any Department workforce member learns, or has reason to believe, that there has been a breach of the security of any of the Department's computer systems, (s)he must immediately notify the Information Security Officer, who will then notify the Director(s) of the affected Division(s) and the Director of Information Resource Management. A breach of the security of a system includes unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the confidentiality or integrity of PPSI maintained by the Department. Good faith acquisition of PPSI by an employee or agent of the Department for the purposes of the agency is not a breach of the security of the system, provided that the private information is not used for unauthorized purposes or subject to unauthorized disclosure. This notification shall be made in the most expedient time possible and without unreasonable delay.

Investigation of reported security breach. The Division Director, the Information Security Officer and the Director of Information Resource Management, will investigate the reported security breach to determine the nature and extent of any such unauthorized acquisition of PPSI. In determining whether information has been acquired, or is reasonably believed to have been acquired, by an authorized person or a person without valid authorization, the Department may consider indications of the following factors, among others:

1. The information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or
2. The information has been downloaded or copied without authorization; or
3. The information as used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

If encrypted data is compromised along with the corresponding encryption key and encryption software, the data shall be considered unencrypted and information will be considered compromised through unauthorized access.

Notification to New York State residents. At the conclusion of the investigation, if it is determined that a security breach of the Department's computer systems occurred, or is

reasonably likely to have occurred, and that the identifying personal information of one or more New York State residents may have been acquired by an unauthorized person or persons, the Information Security Officer will present the findings of the investigation in writing to the Commissioner or designee of the Commissioner, who shall notify the affected New York State residents.

If a third party maintains information on behalf of the Department and identifying personal information is compromised, the Department or the third party will notify the individual of the compromise.

Method of notification. The notice will be provided directly to the affected persons via 1) written notice, 2) electronic notice if the affected person has expressly consented to receiving the information in electronic form, or 3) telephone notice. If the cost of providing notice would exceed two hundred fifty thousand dollars, or if the affected class of subject persons to be notified exceeds five hundred thousand, or if the Department does not have sufficient contact information to provide direct notice, then upon the approval of the Office of Attorney General, substitute notice may be provided. Substitute notice shall consist of all of the following:

(1) e-mail notice when such state entity has an e-mail address for the subject persons;

(2) conspicuous posting of the notice on such state entity's web site page, if such agency maintains one; and

(3) notification to major statewide media.

Notifications will be made as soon as possible after the Department's internal investigation is complete, but may be delayed if a law enforcement agency determines that the notification might impede a criminal investigation.

Content of notice. Such notifications shall include 1) Department contact information, 2) a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, and 3) the elements of identifying personal information that were, or are reasonably believed to have been, acquired by a person without valid authorization.

The Department will notify the Office of Attorney General, the Consumer Protection Board, and the Office of Cyber Security and Critical Infrastructure Coordination as to the timing, content and distribution of the notices and approximate number of affected persons. If more than 5,000 residents are to be notified at one time, the Department shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such additional notices shall be made without delaying the notice to the affected New York State residents.

SAMPLE NOTICE TO NYS RESIDENTS

Name
Address
City, State Zip

Dear :

We are writing to you because of a recent security incident at the NYS Department of Civil Service.

A. The nature of the incident is as follows:
B. The incident may have involved the following types of private information:
C. The Department of Civil Service is taking the following actions to protect against this type of incident in the future:

To protect yourself from the possibility of identity theft, we recommend that you take the following steps:

If credit card or other financial account information is indicated above, you should immediately contact your credit card or financial account issuers and inform them that an unauthorized person may have your account information.

If a Driver's License or Non-Driver's ID number is indicated, immediately contact your local office of the NYS Department of Motor Vehicles to report the theft.

In all cases, to further protect yourself we recommend that you place a fraud alert on your credit files. A fraud alert informs creditors to contact you before opening any new accounts in your name. Contact the three credit reporting agencies at a number below. You will then be able to receive a free copy of your credit report from each.

Experian: 888-397-3742
Equifax: 800-525-6285
TransUnion: 800-680-7289

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information that is not accurate, such as home address and Social Security number. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

For more information on identity theft, we suggest that you visit the Web site of the New York State Consumer Protection Board [www.consumer.state.ny.us]or call them at (518) 474-8583 or (800) 697-1220. Information regarding identity theft is also available from the Federal Trade Commission at www.consumer.gov/idtheft.

If there is anything that the Department of Civil Service can do to assist you, please call **[toll-free phone number**].

Sincerely,

PLEASE SUBMIT THE FOLLOWING FORM TO ALL THREE (3) STATE AGENCIES as follows:

Fax this form to the Consumer Protection Board (CPB):

Security Breach Notification
Fax: 518-474-2474

Also Fax & Mail this form to:

NYS Office of Cyber Security and Critical Infrastructure Coordination (CSCIC):
30 South Pearl St. Floor P2
Albany, NY 12207
Fax: 518-474-9090

Office of the Attorney General
Asst. Attorney General in Charge
Bureau of Consumer Frauds
120 Broadway - 3rd Floor
New York, NY 10271
Fax: 212-416-6003

New York State Department of Civil Service
Report of
"Breach of the Security of the System"
Pursuant to the Information Security Breach and Notification Act (State Technology Law §208)

Name of State Entity:
Date of Discovery of Breach:
Estimated Number of Affected Individuals:
Date of Notification to Affected Individuals:
Manner of Notification: [ ] written notice
[ ] electronic notice (email)
[ ] telephone notice

Are you requesting substitute notice? [ ] Yes [ ] No (If yes, attach justification)

Content of Notification to Affected Individuals: Describe what happened in general terms and what kind of information was involved. Please attach copy of Notice.

Name of Contact Person:
Title:
Telephone number:
Email:
Dated:
Submitted by:
Title:
Address:
Email:
Telephone:
Fax:

Refer to *Security Incident Response and Management Policy*.

DEFINITIONS

Private information: Personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired: (1) social security number; (2) driver's license number or non-driver identification card number; or (3) account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account. Private information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

PPSI: Personal, private or sensitive information**.**

Third Party: Any entity, such as state agency, department, office, division, board, bureau, commission, vendor that is not governed by the Department of Civil Service. Department of Civil Service workforce members are not third parties.

REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA), Security Regulation, Privacy and Security Regulation
- New York State Cyber Security Policy P03-002
- Information technology – Code of practice for information security management, ISO/IEC 17799
- New York State Information Security Breach and Notification Act (New York State Technology Law Section 208)

Policy Name	BLACKBERRY DEVICES
Category	Security
Policy Number	1.25
Policy Owner	Information Security Officer (ISO)
Policy Level	Department
Effective Date	October 1, 2007
Revision Date	October 1, 2008

PURPOSE

To ensure that guidelines and security controls are in place for the issuance of all personal digital assistant (PDA) devices including Blackberries within the Department.

POLICY STATEMENT

The Department recognizes the importance of utilizing new communication technologies to enable workforce members to increase their productivity and efficiency while away from the office. Blackberry devices used in conjunction with the Blackberry Enterprise Server can give Department staff the ability to maintain e-mail contact with co-workers, to access and update their calendars, and to provide access to limited Department applications while away from the office. To ensure that the security and confidentiality of Departmental data and communication is protected and the investment in these devices provides the maximum benefit to the Department, the following guidelines will be followed.

Assignment of Blackberries

Only Department owned and assigned PDA devices will be used to access Department resources. No personally owned devices will be allowed, since the Department has no control over the security on these devices, and any DCS data downloaded to them may be susceptible to interception, theft or loss.

The cost of procuring, supporting and maintaining these tools is significant. Assignment of these devices to workforce members should be carefully considered and based on business need. The following factors, at a minimum, will be considered in evaluating any request for assignment of a Blackberry:

1) The amount of time spent outside of the office.
2) The applications, e.g., e-mail, calendar, or other, that the employee needs access to while outside of the office.
3) The impact of not having access to the needed applications while outside of the office.
4) The availability of the wireless services in the location where the requesting employee will be using while outside of the office.
5) The availability of less expensive alternatives, such as remote access to the Department network from a home computer.

Blackberry users must have a legitimate business need and all requests for this equipment must be approved by their manager, the applicable Division Director, the CIO and the ISO.

Security and Passwords

The New York State Information Security Policy requires that all PDA devices must be encrypted. All PDA devices will now require the password and the content protection options to be enabled.

The Blackberry will have an initial password that Desktop Support issues in order to activate the device. The password option must remain enabled. Users will have the ability to change their password under the security settings, however all other settings must not be changed. This password is in addition to, and different from, the employee's normal passwords used to log into the Department network and to access applications. To protect Department data in the event that the device is lost or stolen, the Blackberry will go into a locked mode after a set period of inactivity, and the password will be needed to unlock it.

The Desktop Support Unit will maintain a list of Blackberry users and their device serial numbers. The employee assigned a Blackberry device must not communicate their password to anyone else. In the event the employee forgets the password, the employee must notify the Help Desk for a password reset. In some instances, the Desktop Support Unit can reset the password remotely and the employee will be notified of the new password. Otherwise the Blackberry will have to be returned to the Desktop Support Unit for a password reset. After 5 incorrect password attempts the user must type **blackberry** in order to continue. After 10 incorrect password attempts, all data will be erased from the Blackberry and the unit must be returned to the Desktop Support Unit for reinitialization of the device.

Rules of Use

When PDA devices are used in public places, care must be taken to avoid the risk of unauthorized persons viewing information on the screens. Such equipment must not be left unattended and must be physically locked when not in use. Workforce members must not check these devices in airline luggage systems. These devices must remain in the possession of the traveler unless other arrangements are required by federal or state authorities.

Lost devices

Should a device become lost or stolen it is imperative that the Help Desk (485-1618) be notified immediately so that the device can be deactivated and disallowed from accessing the Department network.

REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA), Security Regulation, Privacy and Security Regulation
- New York State Cyber Security Policy P03-002
- Information technology – Code of practice for information security management, ISO/IEC 17799
- New York State Information Security Breach and Notification Act (New York State Technology Law Section 208)