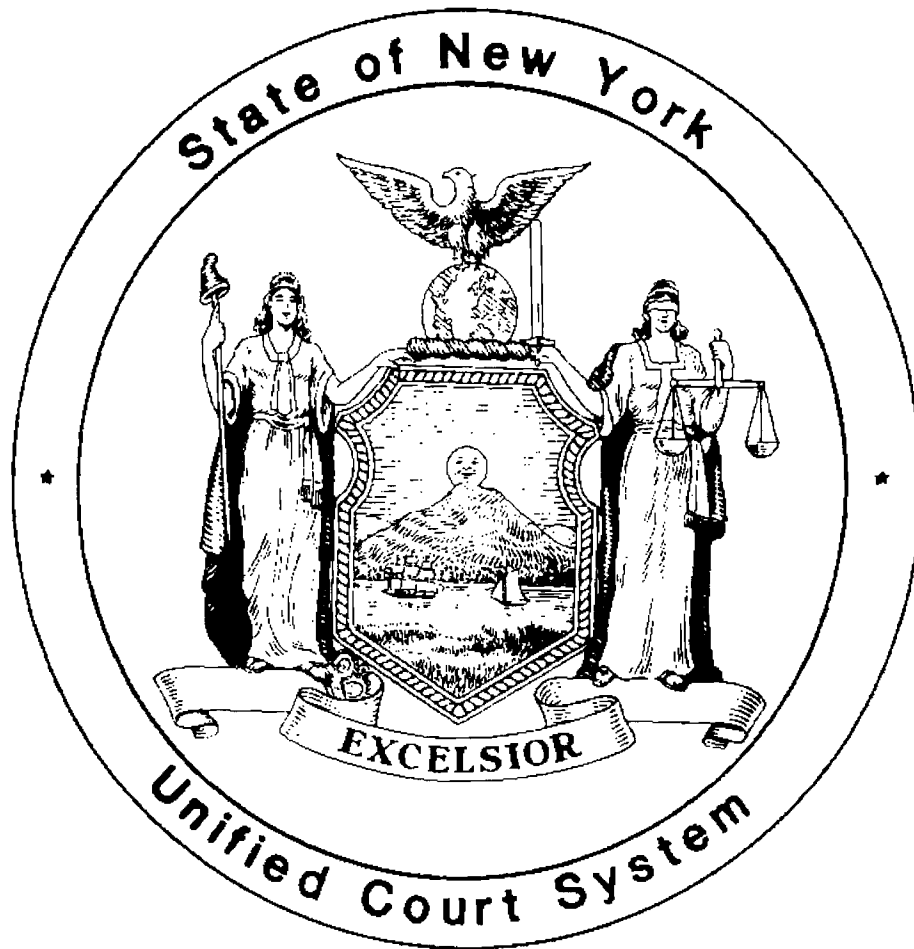


APPENDIX A

**STATE OF NEW YORK
UNIFIED COURT SYSTEM**

DEPARTMENT OF PUBLIC SAFETY



**BUILDING EVACUATION
PLAN**

CONFIDENTIAL

UF103
Revised 12/01

**UNIFIED COURT SYSTEM
DEPARTMENT OF PUBLIC SAFETY
BUILDING EVACUATION PLAN**

PURPOSE: The express purposes of the Building Evacuation Plan is to have available an all inclusive source document which will prove invaluable in planning for contingencies of an immediate nature which may involve complete or partial building evacuation. It is incumbent upon those responsible for security to be prepared to meet emergencies by thoughtful planning, effective training and an overall posture of alertness and forethought.

RESTRICTED: The information contained in the building evacuation plan is confidential. Disclosure to unauthorized persons could result in a compromise of security. Keep this plan properly secured.

**PART I
(INTRODUCTION)**

a. Building Name _____ County _____

b. Building Address _____

c. Courts and other Agencies Located Within Building

	Court/Agency	Telephone
1.	_____	_____
2.	_____	_____
3.	_____	_____
4.	_____	_____

d. Official(s) Authorized to Order an Evacuation

	Title	Department	Telephone
1.	_____		
2.	_____		
3.	_____		
4.	_____		

e. Plan Prepared by:

Name: _____

Title: _____

Telephone: _____

Date: _____

f. Building Owned/Operated By:

<input type="checkbox"/>	City	<input type="checkbox"/>	County
<input type="checkbox"/>	State	<input type="checkbox"/>	Other

_____ **Specify**

g. Number of Floors in Building: _____

h. Number of Floors in Building: _____ **Floor Numbers** _____

i. Number of Floors Occupied by Other Agencies _____ **Floor Numbers** _____

j. Number of Elevators _____

k. Approximate Daily Building Population _____

l. List All Public Entrances & Other Access Points _____

m. List All Private Entrances _____

n. List Any Special Facilities for Person with Disabilities _____

o. Are any Structural Changes Planned for the Building? _____ **Yes** _____ **No**

If yes describe. (Include dates of construction & impact on evacuation plans).

p. Names of Police Agency Having Patrol Responsibility for Court Building

_____ **Precinct/Command** _____

Telephone _____

q. Date of Last Fire Inspection: _____

Inspecting Department: _____

Inspection Findings: (Violations, recommendations, etc. Include any corrective action taken.)

r. Date of Last Fire Drill: _____

s. List Fire Drill Schedule _____

t. List Fire Warden Posts and Areas of Responsibility

1. _____ 2. _____

3. _____ 4. _____

FIRE WARDEN: Designated Individual(s) assist building management in matters of fire prevention and protection. Supervise and expedite the movement of personnel through or out of their assigned area of the building to a predetermined safe location during fire drills and fire emergencies. Fire Wardens shall be designated by work station to cover court facility floors (e.g. officer assigned to mag post or Deputy Chief Clerk in Room 104). A status roster of all Fire Wardens and Deputy Fire Wardens must be maintained daily and made readily accessible on-site!

u. List Name of Bomb Incident Coordinator: _____

List Name of Alternate Coordinator: _____

BOMB INCIDENT COORDINATOR: Designated individual prepares, maintains and updates emergency plans, organizes and trains search teams, establishes and maintains liaison with emergency response agencies and building tenants. Inspects building to prevent/correct safety hazards. Maintains communications with court administrators, security and building personnel, etc. Directs building searches and evacuations as required. The Alternate Coordinator assists in the above activities and acts as a Bomb Incident Coordinator in the absence or incapacitation of the Coordinator.

v. List Building Search Teams:

Search Teams: Designated individuals search assigned areas for suspicious packages devices, order all persons, except those authorized to remain, to leave the vicinity. Search Teams assist in complete or partial building evacuation, notify supervisor or emergency conditions as they develop, provide assistance to fire, police or other emergency personnel as required.

Name	Area of Responsibility
------	------------------------

_____	_____
_____	_____
_____	_____

w. Is Facility Equipped with Emergency Lighting? _____ Yes _____ No

If Yes, Describe _____

x. List Communication Systems Available for Use: _____

y. List Locations of Emergency Command Center _____

z. List Location of Pre-Determined Evacuation Site for Administrative Judges,
Court Administrative Staff and Chief Clerks.

Facility _____

Room No. _____ Telephone No. _____

**PART II
(NOTIFICATION)**

a. List All Court Officials to be Notified:

	Title	Telephone
1.	_____	_____
2.	_____	_____
3.	_____	_____
4.	_____	_____
5.	_____	_____
6.	_____	_____
7.	_____	_____

b. List All Local Agencies to be Notified

1. **Police Dept.** _____
2. **Fire Dept.** _____
3. **EMS** _____
4. _____

d. CHAIN OF COMMAND

Establish Chain of Command During Building Evacuation _____

e. EMERGENCY EQUIPMENT

Identify Type and Location of All Emergency Equipment _____

**PART IV
(LOCAL FIRE CODES)**

A. Attach Copies of Pertinent Local Fire Codes.

**PART V
(FLOOR PLANS)**

- a. Attach Copies of Facility Floor Plans**
 - 1. Identify Those Area Occupied by Court Facilities.**
- b. Attached Exterior Photos of Building (if available).**

**PART VI
(REVIEW AND CERTIFICATION)**

- a. Completed Plan Submitted to:
(filled out by Submitting Court)**

Name

Title

Date

- b. Completed Plan Reviewed By**

Name

Title

Date

c. Plan Reviewed By:

Department of Public Safety

Date

d. Describe Any Action Taken:

APPENDIX B

Building Evacuation Procedures

Interim -- November 14, 2001

The following building evacuation procedures and protocols shall be followed in the event an evacuation of a court facility or portion thereof is ordered in response to a fire or bomb incident or other hazardous condition. In multi-tenant facilities, efforts should be made with other tenants to develop an agreed upon evacuation plan.

Decision to Evacuate

- The decision to evacuate a court facility or portion thereof shall be made by the Administrative Judge, or designee, in consultation with local fire and law enforcement personnel, UCS uniformed supervisors, contractual security personnel and other appropriate local officials.
- Once an evacuation is ordered, it is mandatory. Failure or refusal to evacuate by individuals endangers the safety of emergency response personnel and the general public.

Communication of an Order to Evacuate

A decision to evacuate shall be communicated either by sounding of the fire alarm or by verbal orders to appropriate UCS uniformed supervisors, local law enforcement or contractual security personnel.

Evacuation Procedures

- In multi-tenant facilities, all other tenants must be promptly notified of the court system's decision to evacuate.
- Fire Wardens must be assigned to cover the floors of the court facility. A status roster of all Fire Wardens and Deputy Fire Wardens must be maintained daily and made readily accessible on-site.
- Fire Wardens will select the safest exit to be used for the evacuation.

• These interim procedures have been developed to assist in ensuring the safety, health and security of court system employees and facilities. These interim procedures reflect the current understanding of potential threats and the most recent recommendations from expert law enforcement and fire departments. These interim procedures are subject to change as necessary to reflect any changes in this expert information and advice.

(Elevators may not be used except by fire department personnel. Elevators will automatically descend to the ground floor when the building's fire alarm is activated, unless the alarm originated on the ground floor.)

- Fire Wardens will make exit selections based on the nature of the emergency, i.e. whether it is a fire, bomb, or incident involving hazardous materials. **Fire Wardens will check the safety status of the exit prior to entry by individuals for evacuation.** If the exit is unsafe or obstructed, an alternative exit must be selected.
- Fire Wardens will ensure that all occupants are notified of the incident and that the evacuation is conducted in an orderly manner. Fire Wardens will immediately notify the Fire Command Station or Command Post if an evacuation can not be conducted from a floor or area for any reason.
- The most critical area to be immediately evacuated is the floor on which the incident originated and the floors immediately above and below that floor.
- Patrol Units will immediately commence a thorough search of the facility and assist with evacuation procedures.
- The last person exiting a room or office during an evacuation should close the door without locking it.
- Administrative and Supervising Judges, Court Administrative Staff and Chief Clerks. These individuals will evacuate to a location pre-determined by the Administrative Judge, in consultation with the Chief Clerk and on-site security personnel. It is important that these individuals remain in communication throughout the evacuation, using cell phones, radios (if available and appropriate), telephones, etc.
- Incarcerated defendants. These individuals shall be returned promptly to the holding cell area and will remain in the care and custody of the appropriate custodial agency (e.g., Sheriff, Department of Corrections or local police department). The custodial agency is responsible for the evacuation of those defendants, if necessary.
- Jurors. Sequestered and deliberating juries shall be evacuated, under escort, to a pre-determined location. All other jurors will be evacuated from the facility in the same manner as all other visitors.
- Persons Needing Assistance. Fire Wardens will familiarize themselves with the number and location of persons in their assigned area who may require

assistance during an evacuation. In the event of an evacuation, those needing help should be assembled at the nearest public elevator system. In the event that the fire, bomb or hazardous condition exists at or near the nearest public elevator, these individuals should be moved to a safe fire exit stairwell landing.

A "Buddy System" should be established between each person needing assistance and a co-worker which provides that they will remain together until evacuated.

A current roster of employees who may need assistance with evacuation shall be maintained in each court facility. UCS uniformed and contractual security personnel will be responsible to account for the safety of disabled persons during the evacuation. The decision to evacuate persons who are unable to evacuate without assistance rests with the Fire Department, which will then conduct such evacuation if it is deemed necessary.

- Fire Wardens shall instruct individuals that upon entering a fire exit stairwell they should walk quickly and quietly – **NOT RUN** – toward the EXIT and away from the building.
- Once the evacuation has begun, individuals must not attempt to re-enter the facility or the area until the Fire Department, Police Department / Bomb Squad or Hazardous Materials Unit declare that it is safe to do so.
- Immediately after the evacuation of his or her assigned area, Fire Wardens will report by telephone or radio to the Fire Command Station or Command Post. The report will include the status and location of disabled persons in the Fire Warden's area. Once the area is secured, Fire Wardens and Patrol Units will report to the Fire Command Station or Command Post for further direction.
- Perimeter Control Team. Wherever feasible, a pre-designated Perimeter Control Team, consisting of uniformed / contractual security personnel, will be established by the Administrative Judge, in consultation with on-site security personnel. This Perimeter Control Team will direct and assist in the evacuation effort and in traffic control, pedestrian movement away from the court facility, and restriction of access to the facility.
- Upon leaving the building and at the direction of the Perimeter Control Team if one exists, the public and employees will move at least 1,000 feet from the building to facilitate access for the emergency personnel responding to the incident and to further diminish the risk of harm.

- UCS uniformed supervisors or contractual security personnel shall coordinate with other agency supervisors regarding interior and perimeter activity. All uniformed personnel shall be assigned to pre-determined areas for deployment.

Re-Entry Procedures

- Once the facility or area has been declared safe for re-entry by the Fire Department, Police Department, Bomb Squad, or Hazardous Materials Unit, notification will be given to the appropriate individuals by on-site uniformed supervisors or contracted security personnel.
- The order of re-entry into the facility should be as follows:
 - Uniformed / Contractual Security Personnel
 - Administrative or Supervisory Judges and Administrative Staff
 - Judicial Personnel
 - Court and Agency Employees
 - Jurors and the general public

APPENDIX C



Employee Evacuation Checklist

EVACUATION

IF AN ALARM IS ACTIVATED and/or an EVACUATION IS ORDERED by the Administrative Judge or designee:

- **REMAIN CALM** and follow instructions from the fire/safety wardens and instructions issued on the public address system.
- **TAKE PERSONAL BELONGINGS** (wallets, keys, medication, cell phone, etc.) **ONLY** if they are readily available.
- **IF AT ANY POINT YOU ARE UNSURE** as to how to respond to an alarm, proceed with evacuation.
- **CLOSE INTERIOR DOORS** behind you. Leave doors unlocked as you exit.
- **PROCEED** along the primary **EXIT PATH** to the fire exit stairwell. Direct members of the public to the designated stairway. **DO NOT USE THE ELEVATORS.**
- **PROCEED INTO THE DESIGNATED STAIRWAY** in an orderly fashion using your primary exit pathway. Using handrails, walk, **DO NOT RUN**, to the designated evacuation floor, or, in the event of a building evacuation, proceed down the stairway through the building exit to the designated assembly area.
- **REMAIN ON THE DESIGNATED EVACUATION FLOOR** until directed to return to your office, or, in the event of a building evacuation, remain in the designated assembly area to await further instructions.
- **DO NOT RE-ENTER** the building unless you are instructed to do so by the Fire/Safety Warden or Fire Department.
- In the event of an evacuation, the **DESIGNATED ASSEMBLY AREA** for this building is:

FIRE SAFETY TIPS

- If you discover smoke or fire, immediately activate the nearest fire pull box.
- **FEEL THE DOOR** before opening it. Don't open the door if it's hot. Use an alternate route.
- **IF YOU ARE TRAPPED**, close as many doors as you can between you and the fire, and **SEAL** the cracks with a wet cloth or tape to keep smoke out. If there is a phone, **CALL** the Fire Department (911) to tell them exactly where you are. Otherwise, **WAIT** at a window and try to **SIGNAL** for help with a light colored cloth or a flashlight.
- **DO NOT BLOCK OR WEDGE OPEN STAIRWELL DOORS** during an evacuation. Fire doors leading to stairwells are only effective when they are closed.
- **IF YOU GET CAUGHT IN SMOKE**, get down and crawl. Smoke rises, so there will be cleaner, cooler air near the floor.
- If your clothes catch fire, remember to **STOP, DROP AND ROLL.**

PLANNING

- **IDENTIFY PERSONAL BELONGINGS** (keys, wallets, medication, etc.) that you would take with you in an evacuation and keep them readily accessible.
- **BECOME FAMILIAR WITH THE EMERGENCY EXIT**, fire pullbox locations, evacuation maps, emergency telephone numbers and designated assembly area for your building.
- **PARTICIPATE IN FIRE DRILLS** to become familiar with your building evacuation routes and procedures.
- **KNOW WHO THE FIRE/SAFETY WARDEN IS** for your floor.
- **NOTIFY YOUR FIRE/SAFETY WARDEN** if you have any disability that could delay your escape.

APPENDIX D

**NEW YORK STATE UNIFIED COURT SYSTEM
EMERGENCY PROCEDURES**

- You will be informed by your supervisor or by emergency personnel that an emergency exists.
- Follow local evacuation procedures for your facility.
- In the event of an evacuation, the Designated Assembly Area for your facility is:

■ Decisions on courthouse closings may be different from those for state and local government offices.

FOR INFORMATION IN EVENT OF EMERGENCY

SUPERVISOR'S NUMBERS: _____

OTHER CONTACT NUMBERS: _____

FOR EMERGENCY UPDATES CALL: 1-800-COURTNY
OR VISIT: WWW.COURTS.STATE.NY.US

APPENDIX E



**State of New York
Unified Court System
Department of Public Safety**

MEMORANDUM

**Phase I Evacuation Drill Protocols
Courts Outside New York City**

1. Prior to each evacuation drill, an initial planning meeting is to be held for each facility. The Chief Court Officer, UCS Security Supervisor /Security Contract Supervisor, Designated Security Coordinator and/or Chief Clerk must attend the planning meeting. Administrative and/or Supervising Judges, the Executive Assistant, as well as representatives of major facility tenants may also be invited.
2. The initial meeting is to be followed by a Multi Agency Meeting consisting of representatives of all facility tenants and of local emergency response agencies (Fire, Sheriff, Police, County Emergency Management Office, etc.). Drill logistics and protocols will be reviewed and finalized. Generally, the Chief Court Officer, UCS Security Supervisor/ Security Contract Supervisor, Designated Security Supervisor and/or Chief Clerk shall conduct the meeting.
3. The Chief Court Officer, UCS Security Supervisor/ Security Contract Supervisor or the Designated Security Coordinator shall be charged with notifying neighbors and the business community of the details of the evacuation drill including date, time and scope. Immediately preceding the drill, notices should be posted in and around the facility indicating the date and time of the drill.
4. Local emergency service providers (Fire, Sheriff, Police, County Emergency Management Office, etc.) should be encouraged to participate and assist in assessing the drill.
5. On the day of the drill, after the facility has been evacuated, a head count must be conducted by designated UCS and/or tenant supervisory personnel at the Designated Assembly Areas using time and leave sheets or checklists maintained by supervisors. After the completion of the headcount a final "All Clear" will be given indicating that the drill is over. Depending on when the drill is held and the needs of the court, employees may be dismissed from the assembly area.
6. UCS established protocols for the order of re-entry will be followed.
7. Immediately after each drill, a post action meeting will be held. The Chief Court Officer, UCS Security Supervisor / Contract Security Supervisor, Designated Security Coordinator and/or Chief Clerk shall conduct a critical assessment of the drill, encouraging input from all participants and representatives of local emergency response agencies.
8. A written drill report (UF165) must be completed by the Chief Court Officer, UCS Security Supervisor / Contract Security Supervisor, Designated Security Coordinator and/or Chief Clerk and forwarded to the First Deputy Chief/State Emergency Management Coordinator at the Department of Public Safety. Issues and prospective corrective measures should be identified.

APPENDIX F



**State of New York
Unified Court System
Department of Public Safety**

EVACUATION DRILL REPORT - COURTS OUTSIDE NYC

Facility: _____ Date/Time Drill Initiated: _____

Evacuation Order given by: _____

Present: **Administrative Judge (name):** _____
Executive Assistant: _____
Chief Clerk: _____
UCS Security Supervisor: _____
Contract Security Supervisor: _____
Fire Department: _____
Police/Sheriff's Dept.: _____
Buildings and Grounds: _____
Other (list): _____

Fire Command Station(y/n): _____ Utilized (y/n) _____

Deactivated for drill (y/n): _____

Incident Command Post Established (y/n): _____ (where): _____

Designated Assembly Area(s): _____

All Floors Evacuated (y/n): _____ (If partial evacuation list floors): _____

Floor Deputy Fire Wardens Reporting (note time):

B	1	2	3	4	5	6	7	8	9	10	11

Wardens Failing to Report (list) (reason): _____

All Clear Time: _____ Given by: _____ Agency: _____

Re-entry (y/n/partial): _____ Time completed: _____ Comments: _____

Report completed by: (print / sign)

(OVER)

UF165

This section shall be used to identify issues and plan for corrective action:

Issue (identify): _____

Action to be taken: _____

Issue (identify): _____

Action to be taken: _____

Issue (identify): _____

Action to be taken: _____

Issue (identify): _____

Action to be taken: _____

This section shall be used to identify issues and plan for corrective action:

Issue (identify): _____

Action to be taken: _____

Issue (identify): _____

Action to be taken: _____

Issue (identify): _____

Action to be taken: _____

Issue (identify): _____

Action to be taken: _____

This section shall be used to identify issues and plan for corrective action:

Issue (identify): _____

Action to be taken: _____

Issue (identify): _____

Action to be taken: _____

Issue (identify): _____

Action to be taken: _____

Issue (identify): _____

Action to be taken: _____

APPENDIX G



**State of New York
Office of Court Administration
Department of Public Safety**

FACILITY PROFILE

Page _____ of _____

COURT: _____

FACILITY ADDRESS: _____

COUNTY: _____ # OF FLOORS IN FACILITY: _____

ADMINISTRATIVE JUDGE(S): _____ PHONE: _____

SUPERVISING JUDGE(S): _____ PHONE: _____

CLERK(S) IN CHARGE OF FACILITY: _____ PHONE: _____

UNIFORMED SUPERVISOR(S) IN CHARGE: _____

FIRE SAFETY DIRECTOR: _____ PHONE: _____

LOCATION OF FIRE COMMAND STATION: _____

FACILITY ENGINEER: _____ PHONE: _____

NUMBER OF EMPLOYEES (ALL AGENCIES): _____ JUDICIAL: _____

OTHER: _____

NUMBER OF PUBLIC USERS (AVERAGE DAILY): _____

REGULAR BUSINESS HOURS: _____ NIGHT OPERATION HOURS: _____

OFF HOUR SECURITY PROVIDED BY (explain): _____

COURT AND ANCILLARY AGENCIES IN FACILITY:

Agency Name:	Floors Occupied:	Contact person/phone:

LOCAL POLICE PRECINCT: _____ CO: _____ PHONE: _____

LOCATION OF NEAREST FIRE HOUSE: _____ PHONE: _____

Date Completed: _____ Last Revised: _____ Prepared By: _____



State of New York
Office of Court Administration
Department of Public Safety

FACILITY PROFILE

Page ____ of ____

COURT AND ANCILLARY AGENCIES IN FACILITY:

Agency Name:	Floors Occupied:	Contact person/phone:

COMMENTS: _____

Date Completed: _____ Last Revised: _____ Prepared By: _____

APPENDIX H

Mail and Package Processing Procedures

Interim – November 7, 2001

- I. General Information Regarding the Processing of Mail
 - A. Delivery and Distribution
 1. All mail (e.g. letters, parcels, packages, etc.) delivered to a court facility or office via the U.S. mail service, hand delivery or by commercial carrier (e.g. UPS) must be
 - a. Passed through an x-ray machine, where such equipment is available, and
 - b. Taken to a central non-public area for sorting prior to distribution.
 2. Prior to distribution, all mail must be inspected by hand in an effort to identify and separate any suspicious items. If any such items are identified, follow the procedures outlined in Section II below immediately.
 - B. Protective Equipment and Facility Considerations
 1. The area designated for sorting and opening mail should be situated, if at all possible, in a non-public room
 - a. With a door that closes and locks;
 - b. Outfitted with a telephone or radio with the emergency contact number for the local court security office conspicuously posted on or near it;
 - c. Adjacent to or near by a facility where court system employees can quickly wash their hands or other exposed areas with soap and water.

These interim procedures have been developed to assist in ensuring the safety, health and security of court system employees and facilities, generally and those employees directly involved in the routine processing of mail and packages ("mail"), specifically. These interim procedures reflect the current understanding of potential threats and the most recent recommendations by the Centers for Disease Control and Prevention (CDC) and other expert law enforcement and public health agencies. These interim procedures are subject to change as necessary to reflect any changes in this expert information and advice.

2. **Gloves** – will be provided in a range of sizes, to any court system employee who requests them. The gloves to be provided are made of nitrile, vinyl or butyl rubber; latex gloves should be avoided due to possible sensitivity.
 - a. Those employees who regularly handle mail in any regard should be strongly encouraged to wear the gloves while doing so. As an additional precaution, these employees should be encouraged to wear long sleeves and pants or trousers to minimize the area of exposed skin.
 - b. The gloves are intended for a single-use and should be discarded in the regular trash immediately after all mail is processed without incident. Gloves should not be used if they are torn, have visible holes or any area on the glove appears stressed or irregular. These gloves should also be discarded in the regular trash immediately upon discovery of the irregularity.
 - c. If suspicious mail is identified and handled, all protective gloves of any employee in coming into contact with the mail should be handled as potentially contaminated.

3. **Respirators (Face masks)** – Note, respirators reduce, but do not eliminate exposure to chemical or biological agents and they do not eliminate the risk of contracting illness, disease or infection.

Respirators will be made available to those employees who handle mail and are concerned about reducing the risk of inhaling a chemical or biological agent, provided that the employee:

- a. submitted a signed Medical Questionnaire for Respirator Use which was reviewed and approved by the New York State Civil Service Employee Health Service (employees only need to complete Part A, sections 1, 2 and 3 of the attached form when seeking permission to use a respirator); and
 - b. underwent basic instruction in wearing the respirator as required by the Federal Occupational Safety and Health Administration (OSHA).
 - c. Employees who opt to wear a respirator cannot have facial hair.
4. As a general precaution, all employees should be advised to
 - a. avoid touching skin, eyes or other mucous membranes while handling mail;

- b. thoroughly wash their hands with soap and water when gloves are removed or while handling their mail and, in particular, before eating. Special disinfectant solutions are unnecessary and alcohol-based formulas are not as effective as soap and water.

II. Identification and Processing of Suspicious Mail

- A. Common sense and caution should be used when handling mail. Some characteristics of suspicious mail to keep in mind include, but are not limited to:
 - lopsided or uneven envelopes or packages;
 - excessive weight or postage;
 - unusual stains, discoloration or odor;
 - a mistaken or general-attention address; lack of a return address, an obviously fictitious return address or a return address that differs from the postmark;
 - excessive tape, string or other on-descript wrapping;
 - protruding wires, foil or other obvious mechanical component;
 - audible noises, e.g. ticking; or
 - restrictive endorsement, e.g. "Personal", "Confidential".
- B. If an article of mail is identified as suspicious, the following procedures must be followed with the utmost care and immediacy.

DO NOT

- Panic
- Open the article if it is unopened or reexamine the article if already opened.
- Shake, empty or otherwise disturb the article or its contents
- Move the article to another area or place it in any type of bag.
- Attempt to clean up any contents which may have spilled out of an opened article.
- Wipe hands on clothing in an attempt to clean them. This may only cause the clothing to also become contaminated.

DO

- Immediately cease handling the article.
- If any contents spill out of the article, shut down the HVAC system for the area, if possible. At a minimum, turn off any fans or close any windows to mitigate the likelihood of the

- contents being dispersed.
- Cover the article with anything appropriate and readily available, e.g. a paper, bag, trash can, napkin, tissue, file folder, newspaper, etc.
- Leave the room and, where possible, close the door. However, **DO NOT** leave the immediate area.
- Notify the facilities emergency contact person by dialing the emergency number posted by the phone or radio. (Note that the phone or radio used to place the emergency call should be considered contaminated equipment and treated accordingly.)
- Wash hands and any other exposed area of the skin that may have come into contact with the mail with soap and water.
- Write a list of all the individuals (i.e. employees and visitors) in the room or immediate area where the article was found. Give the list to the emergency personnel who respond, retain a copy for your facility's files and forward a copy to the Office of the Chief of Security.

III. Notification Procedures

- A. Facility Emergency Contact Person(s) – Each court facility must identify the person or persons to be contacted immediately upon the identification of suspicious mail (e.g. the chief clerk, executive assistant, or highest ranking uniformed officer on site). The person will be responsible for determining when law enforcement and public health agencies will be notified of suspicious mail.
- B. All employees must be notified of the identity of their Facility Emergency Contact Person and number and that person's name and number must be conspicuously posted in all areas where mail is likely to be processed.
- C. If law enforcement or public health agencies are notified, the emergency contact person must:
 - i. Immediately contact the Chief of Security at 212.428.2120, and
 - ii. With the assistance of any employee with relevant information, complete and file an incident report.
- D. If hazardous material teams respond to the incident or if hazardous materials are identified, the Emergency Contact Person must immediately notify OCA Employee Relations at 518.474.7537.
- E. If it is confirmed that an employee or employees have come into contact with contaminated mail, immediately contact OCA Employee Relations at 518.474.7537. OCA/ER will act to facilitate medical testing and treatment, where necessary.

On-Site Briefings

Your office should implement these policies immediately. We will be providing on-site briefings covering these procedures and related issues in the very near future and will contact your offices shortly to make the appropriate arrangements.

Please do not hesitate to call me if you have any questions or would like to discuss these procedures further.

encls.

cc: Hon. Joseph J. Trafficanti, Jr.
Hon. Joan B. Carey
Hon. Juanita Bing Newton
Peter J. Ryan, Esq.
Maria Logus, Esq.
Ronald P. Younkens, Esq.
Barbara Mulé, Esq.
Executive Assistants
Chief Clerk, Court of Claims
New York City Chief Clerks
New York City Surrogates Chief Clerks
New York City County Clerks
OCA Assistant Deputy Chief Administrators & Directors
Chief Matthew O'Reilly

APPENDIX I

State of New York



Jonathan Lippman
Chief Administrative Judge

25 Beaver Street
New York, N.Y. 10004
(212) 428-2100

April 10, 2002

To: Administrative Judges
Presiding Judge, Court of Claims

From: Jonathan Lippman *JK*

Subject: *Secure Pass* Court Access Program

As we discussed during yesterday's conference call, OCA will announce today the implementation of the *Secure Pass* program, a new voluntary court access program for attorneys and employees of certain approved governmental and quasi-governmental groups. Presentation of a *Secure Pass* card will allow the cardholder to bypass magnetometer screening, thereby expediting access to the courthouse without compromising security concerns.

The *Secure Pass* card incorporates cutting-edge security features that make the card difficult to duplicate and allow security personnel to easily determine whether a card has been subject to tampering. Applicants will be required to provide high-quality passport photos, which will be imbedded in the cards and then covered with a tamper-resistant hologram. The cards will also include information such as height and eye color, to aid visual verification of identity, and whether the cardholder is licensed to carry a firearm. *Secure Pass* cards will be issued following a thorough application process, including a an electronic criminal history (CRIMS) search of each applicant to determine whether the individual has any criminal convictions or pending charges. The cards will be valid for a two-year period so that all relevant information is kept current.

Attorney application forms and instruction sheets for *Secure Pass* cards will be forwarded to your courthouses by April 19th and should be made available to attorneys, at their request, beginning on Monday, April 22nd. While the process of accepting applications at local courthouses will be substantially the same as the process for current attorney identification cards, detailed instructions will follow under separate

cover from the Division of Administrative Services. In anticipation of a high number of applications at some facilities, please make sure that courthouse staff is adequately assigned as appropriate to keep the lines to a minimum. Cards will be produced internally by the Division of Administrative Services and returned to the local courthouse where the application originated for the applicants to pick up in person. The application fee for attorneys will be \$25 to cover the administrative costs.

Beginning June 4th, this program will be extended to appropriate governmental and quasi-governmental entities housed or regularly conducting business within court facilities. The administrative details of this aspect of the program are still being developed and will involve your input, as different entities are involved at different facilities. Prior to your contacting these entities regarding preliminary plans to include them in the program, as we discussed in the conference call, it would be helpful if you would send a list to Judge Traficanti or Judge Carey of those entities that you have identified for inclusion. This will enable us to formulate a coherent policy for each facility as well as statewide. We anticipate that employees of these entities will be charged a reduced application fee and that the fee will be waived for employees who have undergone a criminal background search as part of their employment application.

In addition to the application packets and instructions regarding the application process, you will also be receiving further information directly from Chief O'Reilly, who will issue detailed *Secure Pass* protocols to assist you and your security staff in implementing the program.

Chief Judge Kaye and I greatly appreciate your efforts and those of your staff and all court personnel in implementing our security procedures and dealing with the public and the bar throughout this difficult time as we have all adjusted to changes in our personal and professional lives. I know we can rely on your support as we continue to work on improving courthouse security and maintaining the proper balance between that security and ensuring access to our courts.

cc: Hon. Joseph J. Traficanti, Jr.
Hon. Joan B. Carey
Hon. Ann Pfau
Hon. Juanita Bing Newton
Chief Matthew O'Reilly
Laura Weigley Ross
Executive Assistants
Chief Clerks

SAMPLE

To be reproduced on government agency or tenant organization letterhead

and submitted with Secure Pass Application at a NYS UCS Facility.

Original signature required.

Date / /

TO: NYS Unified Court System.
FROM: (Organization Executive)
RE: Secure Pass Program Card Application

(For Government Agency Use)

_____ is an employee in good standing with our organization. As a government employee, I understand this individual is eligible for a Secure Pass. I have indicated below whether this individual has undergone a fingerprint criminal history background check conducted by the NYS Division of Criminal Justice Services in the course of their employment with this organization.

(or)

(For Tenant Organization Use)

_____ is an employee in good standing with our organization and is assigned to our office at _____ (court facility address/room #). I understand that this employee, as a tenant in this building, is eligible for a Secure Pass. I have indicated below whether this individual has undergone a fingerprint criminal history background check conducted by the NYS Division of Criminal Justice Services in the course of their employment with our organization.

Should you have any further questions with respect to this application please contact me at (____) _____.

Thank You.

Signature

Print Name

Title

Fingerprint Background
Search Conducted: Please initial

YES _____

NO _____



**State of New York
Unified Court System
Department of Public Safety**

Date: May 3, 2002

Secure Pass Program
Standard Operating Procedures

1. The cardholder must present the Secure Pass Identification Card (the "card") to the officer at the security post.
2. The officer will visually examine the card to ensure that the UCS State Seal hologram is present and intact on the face of the card.
3. The officer must verify the cardholder's identity by comparing the photograph on the card with the individual presenting the card.
4. If the officer has any concern that the photograph on the card is not of the person presenting the card, the officer must confirm identity by closely inspecting the additional information on the face of the card, i.e., height, eye color, and date of birth.
5. If the card indicates that the cardholder is licensed to carry a firearm, the officer must ask the cardholder if he/she is in possession of a firearm. If the response is affirmative, the officer must ensure that the proper steps are taken to store the weapon.
6. The officer must then pass the card under a Ultra Violet scanner to ensure that the UV-encoded Scales of Justice symbols are present and intact on the face of the card.
7. When the officer is satisfied that the card was presented by the individual pictured and described on the card and that the UCS State Seal and the UV-encoded Scales of Justice symbols appear on the face of the card, the card will be returned to the cardholder and access permitted.
8. Bags may be subject to inspection and/or x-ray screening, as circumstances require.
9. The Secure Pass card only allows the cardholder to by-pass magnetometer screening when the cardholder is on official business, rather than appearing in court on a personal matter.



NEW YORK STATE
Unified Court System

SECURE PASS ATTORNEY APPLICATION

New Application
 Renewal
 Replacement

SECTION A - TO BE COMPLETED BY APPLICANT

NAME: _____
FIRST MIDDLE LAST
Please Print Name As It Appears on your Attorney Registration Record.
See Attorney Directory found at: www.courts.state.ny.us

DATE OF BIRTH: _____
MO. DAY YEAR

YEAR OF ADMISSION: _____

FORMER NAME(S): _____

PHONE: _____ E-MAIL: _____

ATTORNEY REGISTRATION #: _____ HEIGHT: _____ FT. _____ INS. EYE COLOR: _____

PROCESSING FEE: \$25.00 (NON REFUNDABLE)

Method of Payment:

CHECK #: _____ PAYABLE TO: NYS OFFICE OF COURT ADMINISTRATION

or

CREDIT CARD:

MASTERCARD VISA

CARD #: _____

Exp. Date: _____

Name on Card: _____ Card Holder's Signature: _____

I, the undersigned, am fully aware that firearms, other weapons and dangerous instruments are not permitted in court facilities. When in possession of any such item, I am required to surrender said item to security personnel for safe keeping while visiting the court facility. (Please Initial) _____

I am licensed to carry a firearm: Yes No

Prior to approval of this application and issuance of a Secure Pass photo ID card, I understand that an electronic search will be conducted to determine whether I have any criminal convictions or pending criminal charges. (Please Initial) _____

I, the undersigned, hereby confirm that I have read and understand the foregoing provisions and agree to all terms and conditions stated therein. I further confirm that the information provided is complete and accurate to the best of my knowledge.

APPLICANT'S SIGNATURE

DATE

SECTION B - TO BE COMPLETED BY THE COURT

Court Facility: _____

PHOTO ID VERIFICATION: TWO (2) REQUIRED
Driver's License: _____ (State) _____ (Number) _____ (Expiration Date)

Passport: _____ (Country) _____ (Number) _____ (Expiration Date)

Other (Government or Employer ID): _____

Passport Photos (2) Attached:

PAYMENT METHOD: Check Credit Card

Processed By: _____
PLEASE PRINT EMPLOYEE NAME

EMPLOYEE SIGNATURE

SECTION C - TO BE COMPLETED BY OCA

- APPLICATION DENIED:
- ___ Incomplete (Explanation) _____
 - ___ Attorney Registration Delinquent (Contact Attorney Registration - 212-428-2800)
 - ___ Card Previously Issued (Attach Copy of Police Report Reporting Loss)
 - ___ Admission not Confirmed (Attach copy of Certificate of Good Standing)

Original: OCA: Pink Copy : Court Facility; Yellow Copy: Applicant

Crims: _____ ID: _____ Att Reg: _____ Credit Auth: _____

SECURE PASS ATTORNEY APPLICATION INSTRUCTION SHEET

SECTION A – TO BE COMPLETED BY APPLICANT

Section A of the UCS-334 (Secure Pass Application) must be completed by the applicant. Your name as it appears on your Attorney Registration Record and your Attorney Registration Number may be reviewed at www.courts.state.ny.us in the Attorney Directory.

The applicant must provide two (2) color passport photos. **(Note: Photos must have a white or light solid background. Personal photographs or photos with colored or cluttered backgrounds will not be accepted.)**

All applicants must appear in person at a New York State Unified Court System facility to submit the application. At that time **two (2) forms of photo ID must be presented** to verify identity. Acceptable forms of photo ID are a valid passport, driver's license, other government-issued or employer-issued photo ID.

A processing fee of \$25.00 for each card must be supplied at the time of application. Acceptable forms of payment are: check or money order, payable to **NYS Office of Court Administration**, or MasterCard or Visa. If the applicant is licensed to carry a firearm, a copy of the firearm permit **must be attached** to the application. If the applicant may carry a firearm based on being a police or peace officer, a copy of the employer ID indicating police or peace officer status **must be attached**.

Applications for Renewal – follow above directions

Application for Replacement – follows above directions and must attach a copy of the police report indicating the loss or theft of the original card.

The card must be picked up personally by the applicant at the court facility and will be released only after verification of identity in the form of a photo ID.

SECTION B – TO BE COMPLETED BY THE COURT

Section B must be completed by an authorized court employee including verifying identity of the applicant with acceptable forms of photo ID

The court employee must verify the information supplied in Section A for completeness and legibility.

The application, photos and payment must be packaged together and forwarded to OCA in a timely fashion, but no less than once per week. The photos and check if applicable should be placed in the envelope provided and the envelope stapled to the application. Care should be taken to avoid stapling through the check or photos.

Upon completion of review and processing, an ID card or denied application will be returned to the originating court facility.

The card must be picked up personally by the applicant at the court facility and will be released only after verification of identity in the form of a photo ID.

THIS CARD MAY NOT BE USED BY ANYONE OTHER THAN THE PERSON NAMED ON THE CARD OR BY ANYONE WHO IS NOT IN GOOD STANDING AS A MEMBER OF THE BAR OF THE STATE OF NEW YORK. A PERSON WHO NO LONGER IS IN GOOD STANDING MUST SURRENDER THIS CARD TO THE NEW YORK STATE OFFICE OF COURT ADMINISTRATION. MISUSE OF THIS CARD MAY RESULT IN DISCIPLINARY PENALTIES AS WELL AS ANY OTHER PENALTIES AUTHORIZED BY LAW.



STATE OF NEW YORK
UNIFIED COURT SYSTEM
25 BEAVER STREET
NEW YORK, NEW YORK 10004

JONATHAN LIPPMAN
Chief Administrative Judge

ANN T. PFAU
Deputy Chief Administrative Judge

June 21, 2002

To: Administrative Judges outside of New York City
Presiding Judge, Court of Claims

From: Ann Pfau **AP**

Subject: Secure Pass -- Extended Program

As discussed with Judge Lippman during the recent conference call, OCA is extending the *Secure Pass* program to include tenants of our court facilities and certain other organizations whose employees regularly conduct business with the courts.

The *Secure Pass* card for tenants and other organizations will incorporate the same security features as the existing attorney *Secure Pass* cards, but will be a different color in order to aid security personnel in distinguishing between attorneys, court personnel and these other groups. These *Secure Pass* cards will be issued following a thorough application process similar to the existing process for attorney *Secure Pass* cards, with one exception; applications made under the extended program must be accompanied by an employment letter from the employer as discussed further below.

As with the attorney *Secure Pass*, applications for the extended program cards will be made at the local courthouses. Cards will be produced by OCA's Division of Administrative Services and returned to the local courthouse where the application originated for the applicants to pick up in person. There will be no application fee for these cards; however, there will be a \$25 replacement fee to cover the administrative costs of reproducing a lost card. The cards will also be valid for a two-year period. Application forms and instruction sheets for *Secure Pass* cards will be forwarded to your courthouses next week.

In addition to the application packets and instructions regarding these application processes, you will be receiving further information directly from Chief O'Reilly, who will issue detailed *Secure Pass* protocols to assist you and your security staff in implementing this extended program.

If you have any questions concerning this program, please contact Chief O'Reilly at 212-428-2605.

cc: Hon. Joseph J. Traficanti, Jr.
Peter J. Ryan
Margaret S. Morton
Ronald P. Younkins
Harold Brand, Jr.
Tomme Berg
David Klingaman
Eugene W. Myers
G. Russell Oechsle

Harry Salis
Susan Sharp
Ronald M. Stout, Jr.
David Sullivan
John R. Voninski
Laura Weigley Ross
Chief Matthew O'Reilly
First Deputy Chief Jewel Williams
Deputy Chief Tom Leddy

Enclosures

SAMPLE

To be reproduced on government agency or tenant organization letterhead
and submitted with Secure Pass Application at a NYS UCS Facility.

Original signature required.

Date / /

TO: NYS Unified Court System
FROM: (Organization Executive)
RE: Secure Pass Program Card Application

(For Government Agency Use)

_____ is an employee in good standing with our organization. As a government employee, I understand this individual is eligible for a Secure Pass. I have indicated below whether this individual has undergone a fingerprint criminal history background check conducted by the NYS Division of Criminal Justice Services in the course of their employment with this organization.

(or)

(For Tenant Organization Use)

_____ is an employee in good standing with our organization and is assigned to our office at _____ (court facility address/room #). I understand that this employee, as a tenant in this building, is eligible for a Secure Pass. I have indicated below whether this individual has undergone a fingerprint criminal history background check conducted by the NYS Division of Criminal Justice Services in the course of their employment with our organization.

Should you have any further questions with respect to this application please contact me at (____) _____.

Thank You.

Signature

Print Name

Title

**Fingerprint Background
Search Conducted: Please initial**

YES _____

NO _____

Facility Tenants

Tenant applications must be accompanied by an employment verification letter from their employer, on organization letterhead, over the original signature of an appropriate executive of the organization (e.g., executive director, head of personnel, managing attorney). A template of an acceptable letter is attached and should be provided to each tenant organization to facilitate the application process. Copies of this form letter should also be available to applicants upon request.

Governmental Agencies

Employees of governmental agencies who regularly conduct business within the courts are also eligible to receive *Secure Pass* cards under this extended program. A governmental employee's application also must be accompanied by an employment verification letter previously discussed with respect to tenant applicants.

Not-for-Profit Agencies

Appropriate not-for-profit agencies whose employees regularly conduct business within the courts may be eligible for inclusion in the extended program. These organizations will be required to submit a letter to Chief Matthew O'Reilly, UCS Department of Public Safety, requesting approval to participate in the program. The letter should state the nature of the organization's business, the title(s) and number of employees who regularly conduct business within the courts, and whether those employees were subject to a criminal history search by fingerprint analysis as a condition of their employment. Chief O'Reilly, after consultation with Judge Carey and Judge Lippman, will determine whether an organization should be approved to participate and will notify the organization by letter of the decision.

If a not-for-profit organization is approved to participate in this program, each employee seeking a *Secure Pass* card must apply individually. Instructions on the card application process and a template employment verification letter similar to that required by tenant and governmental agency applicants will be forwarded to the organization with notification of their approval and must accompany each employee's application. A copy of that form letter is also attached to this memorandum. A list of all not-for-profit organizations approved for participation in this program will be maintained by UCS Department of Public Safety.

Waiver from Participation

An Administrative Judge may request that a specific facility be waived from participating in this extended *Secure Pass* program. Requests for waivers should be facility specific and made in writing directly to Judge Traficanti. Judge Traficanti will review the application and make a recommendation on approval to Judge Lippman, who will decide whether a waiver is warranted.

APPENDIX J

**NYS Unified Court System
Division of Technology
CourtNet Security Policy**

Table of Contents

I.	Introduction	1.
II.	Purpose	1.
III.	CourtNet Information Security Mission Statement	1.
IV.	CourtNet Information Security Mission Objectives	2.
V.	Risk Assessment	3.
VI.	User Log-In (Warning) Banner	3.
VII.	Computer System Hardware, Software, Data, and Services	
	A. General Security Policy Considerations	4.
	B. Access Restrictions and Disclosures	6.
VIII.	Passwords	8.
IX.	CourtNet Security - Standard Operating Guidelines	
	A. Operating Practices Guidelines	9.
	B. Application Developer Guidelines	10.
	C. Internet Guidelines	10.
X.	System Access	
	A. Connections With Outside Sources	11.
	B. Connections With Non-UCS Entities Physically Connected to CourtNet	12.
	C. Connections With Non-UCS Entities Not Physically Connected to CourtNet	13.

Table of Contents Continued

D.	Wireless Connections	14.
E.	Video Conferencing Connections	15.
XI.	Physical Access	15.
XII.	Reporting Security Breaches	16.
APPENDIX A.	18.

**NYS Unified Court System
Division of Technology
CourtNet Security Policy**

I. Introduction

CourtNet is a statewide intranet network providing information transport, services (including Voice-over IP) and access to applications for and between state and local courts, district and administrative offices and other select entities. CourtNet, the information available on it and the services provided by it, is vital and critical to the operation of the Unified Court Systems (UCS). The confidentiality, integrity, and availability of all information and services available on CourtNet are essential to the functioning of the Unified Court System. Therefore, CourtNet's infrastructure must be protected against all threats, either intentional or accidental. Those organizations and individuals that will use CourtNet, make up the CourtNet community. The CourtNet community has delegated the responsibility of providing a secure, trusted environment for its users to the UCS Division of Technology (DoT). In this role, the DoT will manage information security on CourtNet based on the needs of the CourtNet community.

The CourtNet Information Security Policy places specific security responsibilities on those organizations and individuals that desire to connect to CourtNet. In order to support their usage of CourtNet, DoT will provide guidance to the participating organizations and individuals in order to assist them in the connection process and to facilitate their learning and understanding of this security policy and associated compliance requirements.

II Purpose

Effective information security is a team effort involving all those who come in contact with information and/or information systems. In recognition of the need for teamwork, this policy identifies responsibilities and duties associated with information, transport, and services security. These policies provide a framework for making appropriate decisions for implementing information security on CourtNet.

III CourtNet Information Security Mission Statement

Various security mechanisms are used to protect the integrity, availability, and confidentiality of information systems and are an integral part of any organization where sensitive information is stored. With the rapid expansion of technology, system resources can be exposed to numerous threats that can have a negative impact on an organization. Common threats to systems include, fraud and theft, employee sabotage, malicious hackers, software viruses, and threats to personal privacy.

The CourtNet information security mission therefore, is to safeguard the confidentiality, integrity, and availability of information and services on CourtNet.

Within the scope of this mission, confidentiality, integrity, and availability are defined as:

Confidentiality: Information on the CourtNet is not disseminated beyond those who are authorized to access it.

Integrity: Information on the CourtNet retains its original level of accuracy and has not been exposed to accidental or malicious alteration or destruction.

Availability: The CourtNet infrastructure will be accessible by any users who are authorized and inaccessible by any users who are not authorized.

IV CourtNet Information Security Mission Objectives

In order to accomplish the CourtNet information security mission the following objectives must be met:

1. Establish an evolutionary, risk managed information security program that defends against internal and external threats.
2. Establish a management structure that addresses the operation of CourtNet information security.
3. Require that managers, developers, administrators, technicians, contractors, and users who are exposed to CourtNet:
 - a. be knowledgeable of acceptable CourtNet usage, and
 - b. understand their information security responsibilities.
4. Support and assist entities in understanding and complying with CourtNet Information Security Policy.
5. Establish a routinely performed probing of vital CourtNet points of information and access to determine whether or not safeguards and protections are working.
6. Establish a routine review of log files that audit the access of information to discern whether or not safeguards and protections are working.

V Risk Assessment

A risk assessment must be performed on all applications and services to be deployed on systems and networks on CourtNet. Any organization, unit, or individuals that deploys an application or service on CourtNet is responsible for performing this assessment. The results of this assessment must be delivered in writing to the CourtNet Security Administration prior to introduction of the application or service on CourtNet. As part of this assessment, all application development must ensure that programs contain the minimum security elements outlined in the policy - i.e. unique user ID, ability to change password etc.. Each organization, unit, or individuals that deploys an application or service on CourtNet will also provide regular reviews and updates of this assessment.

This assessment should include:

1. identification of threats and vulnerabilities;
2. identification of application and information owners;
3. analysis of the value of information; and
4. identification of the business impact of security compromises.

VI User Log-In (Warning) Banner

At sign-on, all applications must provide a "warning banner" which will advise the user of unauthorized use, possible penalties, and responsibilities for continued use. A suggested banner is as follows:

Notice

- This system and all data are the property of the New York State Unified Court System (UCS).
- Unauthorized use or attempted unauthorized use of this system is not permitted and may constitute a crime. Such use may subject you to appropriate disciplinary action, criminal and/or civil penalties.
- Use of this system is only permitted by specific authorization of the UCS.

The use of computers, e-mail and the Internet by employees, agents and contract staff of the UCS is subject to UCS policies. Use is limited to conducting official business involving the UCS.

Any use, authorized or not, constitutes an expressed consent for authorized personnel to monitor, intercept, record, read, copy, access or capture such information for use or disclosure in any

manner without additional prior notice. Users have no legitimate expectation of privacy during any use of this system or of any data or information on this system. If you continue, it will mean that you have read and accept the above terms and conditions.

VII Computer System Hardware, Software, Data, and Services

A. General Security Policy Considerations.

1. It is UCS policy that all UCS computer resources (hardware, software, data and services) will only be used for purposes directly related to the business of the Courts. Use of these computer resources for personal purposes is prohibited.
2. All computer equipment including hardware, software, services and related items (excluding supplies) connected to CourtNet will meet UCS standards and must be pre-approved by the UCS Division of Technology.

Personal copies of software or personally acquired hardware devices are not allowed to execute or reside on UCS computer systems, even if they have been obtained legally, without prior written approval from DoT's Security Administration Unit.

The judiciary and non-judicial staff may not bring their own computers, computer peripherals, or computer software into UCS facilities without prior approval from a supervisor. Connection of non-UCS computers, peripherals, or computer software to CourtNet requires both approval from a supervisor and prior written approval from DoT's Security Administration Unit.

3. Any use of storage space or media for personal purposes is deemed inappropriate and is prohibited.
4. UCS will not be liable for any loss or damage resulting from the use of personally-owned computer hardware or software in the work environment.
5. All users will respect and protect others' privacy and confidentiality.
6. All users must comply with UCS and unit policies, procedures, and standards.

Users refers to UCS employees, approved contractors, and any workers from entities outside of UCS who are using, with prior approval, or have access to UCS resources.

7. The Internet connection and services are provided for employees and persons legitimately affiliated with the UCS for the efficient exchange of information and the completion of assigned responsibilities consistent with UCS' statutory purposes.
 - a. The use of Internet facilities by any employee or other person authorized by the UCS must be consistent with policies and standards governing network and system use.
 - b. The content of anything exchanged via Internet access must be appropriate and consistent with UCS policy, subject to the same restrictions as any other correspondence.

8. Use of e-mail is subject to UCS policy. This policy can be found in the Employee's Handbook or on the Security Administration Unit's CourtNet web page. E-mail services, like other means of communication, are to be used to support UCS business. Staff may use e-mail to communicate informally with others in the UCS so long as the communication meets professional standards of conduct. Staff may use e-mail to communicate outside of the UCS when such communications are related to legitimate UCS activities and are within their job assignments or responsibilities.

E-mail messages sent or received within CourtNet may:

- be releasable to the public under the Freedom of Information Law;
 - require special measures to comply with the Personal Privacy Protection Act;
 - may be subject to discovery proceedings in legal actions.
9. All users must respect the network as a shared resource and be sensitive to the impact of user traffic on network performance.

 10. Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC et seq.), notice is given that there are no facilities provided by the system for sending or receiving private or confidential electronic communications. The UCS has the responsibility to manage, review and monitor electronic communications. System administrators and others may have access to all e-mail and users access requests, and will monitor messages as necessary to assure performance and appropriate use. Messages relating to or in support of inappropriate activities may be reported to the appropriate authorities.

 11. The UCS reserves the right to log network use and monitor file server space utilization by users and assumes no responsibility or liability for files deleted due to violation of file server space allotments.

12. The UCS 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 a user risk.
13. All information published, disseminated or otherwise made available via a connection to the UCS systems or applications must comply with all applicable statutes, regulations and policies.

B. Access Restrictions and Disclosures.

1. Unnecessary browsing of UCS Systems and Networks is prohibited. Workers must not browse through UCS computer systems or networks unnecessarily. For example, curious searching for interesting files and/or programs in the directories of other users is prohibited. Just because information is not protected doesn't imply that access is appropriate or necessary. Steps taken to legitimately locate information needed to perform one's job is not considered browsing.
2. System privileges must be defined so that non-production staff (internal auditors, information security administrators, programmers, computer operators, etc.) are not permitted to update "production" information.
3. Software development staff must not be permitted to access production information, with the exception of the production information relevant to the particular application software on which they are currently working.
4. Comments that employee's post to an electronic mail system, an electronic bulletin board system, or other electronic systems are not necessarily formal statements of, or the official position of, the UCS.
5. UCS uses access controls and other security measures to protect the confidentiality, integrity, and availability of the information handled by computers and communications systems. In keeping with these objectives, management maintains the authority to:
 - a. restrict or revoke any user's privileges,
 - b. inspect, copy, remove, or otherwise alter any data program, or other system resource that may undermine these objectives, and
 - c. take any other steps deemed necessary to manage and protect its information systems. This authority may be exercised with or without notice to the involved users, UCS disclaims any responsibility for loss or

damage to data or software that results from its efforts to meet these security objectives, and

- d. periodically review access to determine if it continues to be required, should be modified or eliminated.
6. Users must not read, modify, delete, or copy a file belonging to another user without first obtaining permission from the owner of the file. Unless general user access is clearly provided, the ability to read, modify, delete, or copy a file belonging to another user does not imply permission to actually perform these activities.
7. Users of the UCS information systems are prohibited from gaining unauthorized access to any other information systems or in any way damaging, altering, or disrupting the operations of these systems. Likewise, workers are prohibited from capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism which could permit unauthorized access.
8. Computer systems handling sensitive, valuable, or critical information must securely log all significant computer security relevant events. Examples of computer security relevant events include: password guessing attempts, attempts to use privileges that have not been authorized, modifications to production application software, and modifications to system software.
9. Upon termination of employment, employees may not retain, give away or remove from UCS premises any UCS information other than personal copies of information disseminated to the public and personal copies of correspondence directly related to the terms and conditions of their employment. All other UCS information in the custody of the departing worker must be provided to the worker's immediate supervisor at the time of departure.
10. Upon the termination or expiration of their contract, all contractors, consultants, and temporaries must hand over to their project manager all copies of UCS information received or created during the performance of the contract.
11. When a worker leaves any position with UCS, both computer resident files and paper files must be promptly reviewed by his or her immediate manager to determine who should become the custodian of such files, and/or the appropriate methods to be used for file disposal. An employee's account will be disabled immediately after he/she departs. However his/her data file stored in PC's or servers will be purged after 30 days unless requested by his/her supervisor. The computer user's manager must then promptly reassign the computer user's duties as well as specifically delegate responsibility for information formerly in the computer user's possession.

12. UCS management reserves the right to revoke the privileges of any user at any time. Conduct that interferes with the normal and proper operation of UCS formation systems, which adversely affects the ability of others to use the information systems, or which is harmful or offensive to others, will not be permitted.
13. By making use of UCS systems, users consent to allow all information they store on UCS systems to be divulged to law enforcement at the discretion of UCS management.
14. Employee's must not disclose to any persons outside UCS either the information system controls that are in use or the way in which they are implemented. Specific information about information systems vulnerabilities, such as the details of a recent system break-in, must NOT be distributed without express authorization by UCS management. Exceptions will be made only if the permission of the Assistant Deputy Chief Administrator is first obtained.
15. Employees entrusted with confidential or propriety information shall restrict access and use to authorized individuals (internal or external) based on need to know to perform job function. Employees cannot engage in other actions to take personal advantage of the information available to them or pass it on to others. User access to information does not imply or confer authority to act as a spokesperson for the UCS concerning such information or to discuss such information with others.
16. All employees are required to comply with federal copyright laws, non-disclosure and vendor licensing agreements governing the installation, use, and distribution of purchased software.

VIII Passwords

All computer systems and all computer applications, including e-mail access, are required to be password protected. All passwords must conform to the following guidelines:

- A. User IDs and Passwords will be unique to each authorized user.
- B. Difficult-to-Guess Passwords.
 1. For all systems residing on or connected through CourtNet, users must choose passwords that are difficult to guess. Passwords must not be related to one's duties or personal characteristics. For example, a car license plate number, a job title, a spouse's name, or fragments of an address must not be used. Furthermore,

a password must not be a word found in a dictionary or some other part of speech. Proper names, places, technical terms, and slang must also not be used.

2. An appropriately constructed password will be at least six characters long composed of randomly selected letters, special characters, and numbers.

A difficult-to-guess password can, at times, also be difficult to remember. A good approach for creating a password that can easily be remembered would be to take the first character from each word in a sentence that only makes sense to the user. For instance, "My two children play at school" would make a password "m2cp@s".

- C. Passwords should be protected at all times. Passwords should not be written or displayed. Passwords should never be shared with co-workers. Passwords should never be provided to any unauthorized personnel.
- D. Password Aging. Passwords must automatically age and expire such that users will be required to periodically change their passwords. All user passwords must automatically expire after a minimum of a sixty (60) day period at which time they must be reset. All applications must provide the user with an ability to change the password. A history file must be used on these systems to prevent the reuse of passwords. The CourtNet Security Administration Unit, in conjunction with the users, application developers, and the CourtNet Security Committee, will determine password-aging requirements.
- E. Password Storage. Passwords must be encrypted when stored or transmitted. Passwords must not be stored in unencrypted form in batch files, automatic log-in scripts, software macros, terminal function keys, computers without access control systems, or in other locations where unauthorized users might discover them.
- F. All vendor-supplied default passwords must be changed upon installation.
- G. All user ids must automatically have the associated privileges revoke after a ninety (90) day period of inactivity.
- H. To prevent password guessing attacks, the number of consecutive attempts to enter an incorrect password must be limited. After three (3) unsuccessful attempts to enter a password, the involved user-id must be suspended until reset by a designated system administrator. If any external network connections are involved, that connection must be disconnected, if possible.
- I. Access to e-mail accounts should always be password protected. When working with important or confidential documents, word processing documents should be password protected. All passwords applied to e-mail accounts or word processing documents should follow the password guidelines as set forth in this document.

IX CourtNet Security - Standard Operating Guidelines

A. The following guidelines should be standard operating practices.

1. No desktops or servers directly connected to CourtNet should have attached modems or any other device that provides for outside connectivity. Any exceptions have to be approved by the Deputy Chief Administrative Judge and such approval forwarded to Security Administration Unit (SAU).
2. All servers and network devices must be configured to have high security.
3. Any default administrator password must be changed and follow standard password guidelines.
4. Rename default administrator account name. Leave administrator ID with low permissions and audit for abuse.
5. Any unused Network services should be disabled.
6. Audit and log all access as required by the application, and periodically review logs for abuse.
7. Network Administrators must keep abreast of security vulnerabilities and apply latest patches.
8. All servers and desk tops must have password-protected screen savers, active after a maximum of thirty (30) minutes of inactivity.

B. Application developer guidelines.

1. All form input checked and limited in order to prevent buffer overruns, especially on Internet web applications.
2. Consideration should be made to put all applications designed for use by non-

CourtNet users on the Internet instead of requiring VPN access to get to the application.

C. Internet guidelines.

The Internet must be considered a hostile network.

1. Any connectivity to the Internet from CourtNet must be through a firewall managed by DoT.
2. Any connectivity to CourtNet from the Internet must be through a firewall managed by DoT.
3. In accordance with Division of Technology guidelines and procedures, all PCs connected to CourtNet must use approved anti-virus software.
New viruses are discovered daily. The effectiveness of anti-virus software is dependent on having the latest virus profiles and definitions installed on your computer so that it can look for recently discovered viruses. It is required that these profiles and definitions are kept up-to-date.
4. It is the responsibility of every user of CourtNet to be aware and vigilant of potential cyber threats. The UCS Division of Technology requires all users of CourtNet to act in accordance with the following practices of safe computing:
 - a. Consult your system support personnel if you work from home. The same precautions and protections that are required in the work place also apply to home use.
 - b. Use virus protection software.
 - c. Use a firewall.
 - d. Don't open unknown e-mail attachments.
 - e. Don't run programs of unknown origin.
 - f. Disable hidden filename extensions.
 - g. Keep all applications, including your operating system, patched.
 - h. Turn off your computer or disconnect from the network when not in use.
 - i. Disable Java, JavaScript, and ActiveX if possible.
 - j. Disable scripting features in e-mail programs.

- k. Make regular backups of critical data.
- l. Make a boot disk in case your computer is damaged or compromised.

X System Access

A. Connections With Outside Sources.

1. As mentioned earlier in this document, CourtNet is the name of the New York State Unified Court Systems internal network or intranet. CourtNet currently connects the majority of court facilities across the state together in a high speed network. There are entities who currently need access to CourtNet resources or services and do not have a physical connection to CourtNet. Some of these entities are:
 - a. State Court facilities not connected to CourtNet.
 - b. Town and Village Justices.
 - c. Criminal Justice and Law Enforcement Agencies.
 - d. District Attorney Offices.
 - e. Legal Aid Societies and Public Defender Offices.
 - f. Federal, State and Municipal Agencies.
 - g. Service Providers and other Court-Mandated Programs and Partner Agencies.
2. Resources or services that are required by outside entities should be reviewed to see whether it is appropriate to make this resource or service available on the Internet. External entity connections to CourtNet should be the exception, not normal policy. The Security Administration Unit, in collaboration with the CourtNet Security Committee, will be responsible for the initial review and approval. Conflicting or controversial requests will be sent to Deputy Chief Administrative Judge for final approval. Some examples of the resources and/or services that are required by these entities are:
 - a. Criminal and Civil Court Appearance history information.
 - b. CourtNet applications, such as Attorney Registration, or CourtNet services, such as on-line forms and informational documents.

- B. Connections with non UCS entities that are physically connected to CourtNet.**
- Some of these entities may have the ability to be physically connected to CourtNet. This could happen if the entity were located in a court building that was connected to CourtNet. Another way this could occur is if a court facility were in another building

(such as a county or state building) where other entities who require CourtNet access may exist. If such an entity were to direct-connect their network to CourtNet (run a wire connecting to CourtNet), they could have access to all of the services and resources available on CourtNet. This also creates an additional security risk in that, potentially, a person from the entity's network could try and break into secure areas of CourtNet. This type of connection to CourtNet is, in general, not allowed without the following conditions being met:

1. A written request must be made to the SAU detailing the following:
 - a. Type of access.
 - b. TCP/IP address and port number of each service/resource being accessed.
 - c. TCP/IP address of each client to connect to CourtNet.

2. The network group must place a firewall between the networks that would only allow the necessary TCP/IP addresses and ports to be accessed.

The type of access will be restricted to the following services.

- a. Telnet access to mainframe applications.
- b. WWW access to applications; i.e. http and/or https.
- c. Specific database and/or application server access.

3. All access will be logged by firewall device. Logs will be analyzed and reports generated monthly.
 - a. DoT Firewall policies should be managed centrally with one management tool.
 - b. Only requested TCP/IP addresses and ports will be allowed.

4. Entities wishing to connect to CourtNet and/or to exchange data with UCS must sign a formal agreement stating that the entity will adhere to agreed-upon security protocols related to accessing CourtNet and business rules governing the use of that data.

- C. Connections with non UCS entities that are not physically connected to CourtNet. Other entities exist that do not have a physical connection to CourtNet and are not physically close to a court facility. For these type of entities who require to access

CourtNet the following is required:

1. All requests for access to CourtNet must be in writing and submitted to the Security Administration Unit for approval. This request will document the service and/or resource required.
2. All connections from outside entities to CourtNet must be over the Internet, through a Virtual Private Network (VPN), using PPTP, IPSec or other software provided or approved by DoT. This will require the entity to have Internet access to then create a VPN connection to CourtNet.
3. Outside entities connecting to CourtNet via VPN must use a firewall. The type of firewall used and a statement of use must accompany an entity's request for access to CourtNet. This firewall can be hardware or software-based, but it must be approved by the Security Administration Unit.
4. Entities wishing to connect to CourtNet and/or to exchange data with UCS must sign a formal agreement stating that the entity will adhere to agreed-upon security protocols related to accessing CourtNet and business rules governing the use of that data.
5. When connecting a CourtNet device or computer to another network, there must be controls in place to ensure that only network traffic explicitly required is allowed. All other traffic must be rejected.
6. VPN logs will be analyzed and monthly reports generated for review.
7. VPN passwords must automatically age and expire after a specified time. Before being renewed, all VPN accounts will be checked for activity. Inactive accounts will be allowed to expire and will not be renewed.

D. Wireless connections.

1. **Wireless Bridge connections.**
Within CourtNet, it is often expedient and cost-effective to establish a wireless connection (i.e., radio) between two site locations that have a clear line-of-sight and are within acceptable distance limits. Such communication equipment must

have at least 128-Bit WEP (Wired Equivalent Privacy) transmission encryption capability and said feature must be enabled.

2. **Wireless LAN connection.**

Within CourtNet, it is occasionally expedient and cost-effective to establish a wireless access point to provide edge connectivity to network devices. Such communication equipment must have at least 128-Bit WEP (Wired Equivalent Privacy) transmission encryption capability and said feature must be enabled.

The factory default Access Point ID must be changed upon installation and changed frequently thereafter in accordance with the established guidelines.

E. **Video conferencing connections with non UCS entities**

Video conferencing presents some different issues when connecting to CourtNet. To accommodate video conferencing a video bridge or multi-port conferencing unit, the "Accord MCC-100", will be used for entities not connected to CourtNet. The "Accord MCC-100" will be connected to the Internet and the external entity will use the Internet to video conference with CourtNet users.

XI Physical Access

Any entity with connection to CourtNet will put into place appropriate safeguards to limit physical access to any computer or computer related devices, including routers and switches. Physical security is a prerequisite to information security. Physical access to such equipment potentially provides access to the information stored therein. Physical security mechanisms can protect CourtNet from both deliberate violations, such as attempts by unauthorized individuals to gain access to system resources, and unintentional interruption, such as accidental damage to hardware, leading to degraded services. Each organizational unit with a connection to CourtNet is responsible for ensuring the proper security for all hardware, software, documentation, data and information that is present at their locations.

A. **Secure Locations.**

Mainframes, servers, PC work stations, laptops and other essential computer devices such as routers and switches, will be stored in a location that protects them from unauthorized physical access.

B. **Location Selection.**

Physical locations for all computer related equipment should be selected to protect equipment against equipment and information loss by flood, fire, disasters, sabotage and

theft.

C. **Review of New Connections to Outside Sources.**

Proposed access to or from an entity external to the UCS must be reviewed and approved for physical access conformance by the Division of Technology prior to establishment of the connection.

D. **Review of Installation.**

Installation, upgrade or changes of computer related devices which are directly connected to CourtNet, must be reviewed by the Division of Technology for potential physical security risks.

E. **Laptop, Notebook, and Portable Computer Devices.**

Portable computing devices must not be left unattended at any time unless the device has been secured. When traveling, portable devices should remain with the employee where possible. All portable devices purchased by a District Office, Court or the Division of Technology must include an appropriate lock/cable for securing the device.

XII. Reporting Security Breaches.

Security is used to protect the integrity, availability, and confidentiality of automated information systems and should be an integral part of any organization. The best weapons for defending against malicious intruders and keeping our work place safe are knowledge and awareness.

Security awareness, understanding the basics of security and knowledge of security policy, is everyone's responsibility. Security breaches can take several forms. The best defense against security breaches are conscientious and alert users. The user is the most important person for early detection and prevention. Examples of breaches include:

- Damage to equipment, facilities, utilities.
- Loss or misplaced media (e.g. disks, tapes, cd, paper) containing confidential or highly restricted information.
- Inappropriate use on the computing environment.
- Unauthorized access or attempted unauthorized access to information, resources or services.

Any misuse of CourtNet computer resources and any breaches or violations of CourtNet Security Policy need to be reported immediately to DoT's Security Administration Unit.

DoT's Security Administration Unit can be reached by calling **1-800-622-2522** or by sending a GroupWise message to Security Administration Unit in CourtNet or Security_Administration_Unit@courts.state.ny.us via internet mail.

Appendix A.

Source References.

1. Comments and documentation provided by the CourtNet Connection Policy Development Committee: Paul Morrell, David Drace, Pete McDonald, Dave Dankanich, Mei-Ling Lo, Daniel Morone.
2. User Security Policy and Procedures, UCS Division of Technology,
3. Security Administration Mission Statement, UCS Division of Technology
4. Internet Policy and Guidelines, UCS Division of Technology
5. DoT Network Security Standards
6. Technology Policy 99-2; Role of the Information Security Officer
<http://www.irm.state.ny.us/policy/99-2.htm>
7. Technology Policy 97-8; NYeNet IP Addressing Policy
<http://www.irm.state.ny.us/policy/97-8.htm>
8. Technology Policy 97-1; Information Security Policy
http://www.irm.state.ny.us/policy/tp_971.htm
9. Technology Policy 99-2; Data Sharing Among Agencies
<http://www.irm.state.ny.us/policy/96-19.htm>
10. *Information Security Policies Made Easy*, Charles Cresson Wood. Excerpts made available by OMRDD and OFT.
11. *Information Security Management Handbook, 4th Edition, Volumes I and II*, Harold F. Tipton and Micki Krause.