

## AGENDA

### COMMITTEE ON ADMINISTRATION/INFORMATION SYSTEMS

December 15, 2009  
Aldermen O'Neil, Garrity, Arnold,  
Pinard, Osborne

3:00 PM  
Aldermanic Chambers  
City Hall (3<sup>rd</sup> Floor)

1. Chairman O'Neil calls the meeting to order.
2. The Clerk calls the roll.
3. Communication from the Highway Department regarding a recommendation on Excavation Permit fees.  
*(Note: Referred by the Board of Mayor and Aldermen on November 24, 2009)*  
**Gentlemen, what is your pleasure?**
4. Communication from Dr. Thomas Brennan, Superintendent of Schools, requesting approval of all expenditures related to the renovation of MCTV studios, if available.  
**Gentlemen, what is your pleasure?**

#### TABLED ITEMS

*A motion is in order to remove any item from the table.*

5. Policies and procedures for compliance with Red Flag, State Statute and Payment Card Industry requirements submitted by Jennie Angell, Director of Information Services.  
*(Note: Attached is a letter from Jane Gile, Human Resources Director, regarding the Sensitive Information Policy and Program. Tabled 11/9/09. Updated information from Jennie Angell on December 1, 2009 has been attached.)*
6. Communication from Jennie Angell, Director of Information Services, updating the Committee on the current status of credit card acceptance and requesting a recommendation from the Committee on moving forward.  
*(Tabled 11/9/09)*

7. Recommendation from Matthew Normand, Acting City Clerk, regarding a policy for street closures and license events.  
*(Tabled 03/16/09)*
  
8. Communication from Thomas Clark, City Solicitor regarding a Naming Rights Policy.  
*(Note: Referred by the Board of Mayor and Aldermen on 2/3/09. Tabled 03/16/09)*
  
9. Communication from Barbara Potvin, New England Sampler, requesting the City hold a public forum to discuss the process of closing off city streets and the impact that these closings have on local small businesses as well as the benefits drawn by the City of Manchester and its local citizens.  
*(Note: Referred by the Board of Mayor and Aldermen on 10/21/08. Tabled 11/24/08 recommendation to be submitted by staff)*
  
10. There being no further business, a motion is in order to adjourn.

Copies sent to BMA 11/2  
-handed out @ 11/24/09

Kevin A. Sheppard, P.E.  
Public Works Director

Timothy J. Clougherty  
Deputy Public Works Director



Commission  
William A. Varkas  
Henry R. Bourgeois  
Joan Flurey  
William F. Houghton Jr.  
Robert R. Rivard  
In Board of Mayor and Aldermen

RECEIVED  
NOV 25 2009  
CITY CLERK'S OFFICE

# CITY OF MANCHESTER

## Highway Department

Date: 11/24/09  
On motion of Ald. Gatsas  
Seconded by Ald. Shea  
Voted to refer to the  
Committee on  
Administration/  
Information Systems.

### EXCAVATION PERMIT FEE RECOMMENDATION

*[Signature]*  
City Clerk

Any Contractor wishing to excavate within the City's public right of way must obtain the proper insurance, a surety bond (see attached description) and an excavation permit prior to beginning the work. An excavation permit is the mechanism used by the Highway Department to control and monitor all excavations within the City's public right of way. By requiring this permit, we endeavor to ensure that all excavations are restored in accordance with the City standards outlined in the "Standard Specifications for Road, Drain and Sewer Construction".

Periodically, it is necessary for the City and Highway Department to review the cost of the Excavation Permit fee to ensure that the Permittee properly reimburses the City for costs incurred by the City. In our review, we have identified two areas of concern. These relate to administrative/engineering/inspection and the cost of roadway degradation. Our current administrative/engineering/inspection cost is \$200 per permit. At this time, our analysis confirms that this amount is consistent for those costs. We **do not** currently charge for roadway degradation, but we are recommending that we begin charging for roadway degradation beginning on January 1st of 2010.

However, whenever a roadway is excavated, degradation occurs. Across the United States, municipalities are realizing that the true costs associated with damage to right of way infrastructure go beyond the costs mentioned above. The American Public Works Association (APWA) has conducted studies which conclude that *"the estimated reduction in the life of a pavement with utility cuts varied from 20% to 56%. The estimated life for pavements without utility cuts ranges from 10 to 30 years, depending on the location"*. In a nutshell, the paper clearly justified the application of fees to offset the cost of reduction in value of the street following an excavation. This is commonly referred to as right of way degradation.

Degradation fees attempt to recover the costs due to pavement degradation (loss of road life due to intrusion of the road surface). Degradation losses are not limited to paved areas, but are also incurred from damage to trees, sidewalks, landscaped areas, and other infrastructure, or amenities located within the right of way.

The APWA outlined how other Cities throughout the nation (for example, Concord, New Hampshire, Shelburne, Vermont, Cincinnati, Ohio, Seattle, Washington and many others) are dealing with pavement degradation and have instituted roadway degradation permit fees to recover costs that are incurred by cities and towns.

In addition, the City of San Francisco conducted a statistical analysis of roadway condition data. The analysis revealed that utility cuts result in a significant, immediate decrease in the condition

of the pavement with the damage being roughly equivalent to several years of normal wear. San Francisco is using this analysis to quantify their pavement damage and has developed policies to finance pavement restoration.

The Department of Highways has adapted the roadway degradation fee principle for the City of Manchester and has developed a fully justified fee structure that we believe to be fair and equitable to the City. **We are recommending that the City maintain our current administrative/engineering/inspection cost of \$200 and add new fees of \$5.00 per square foot of paved areas (both road and sidewalk) located in the R.O.W., and \$1.50 per square foot of unpaved areas located within the R.O.W. These prices should be adjusted on January 1<sup>st</sup> on an annual basis based on the "Consumer Price Index (CPI)" as published by the United States Department of Labor, Bureau of Labor Statistics. The "Excavation Permit Fee Calculations" are attached.**

**Surety Bond Description:**

Surety Bond requirement from Standard Specifications for Road, Drain and Sewer Construction:

*The permittee agrees to furnish a continuing surety bond in the amount of five thousand dollars (\$5,000) to guarantee the fulfillment of the provisions, instructions and regulations of the permit.*

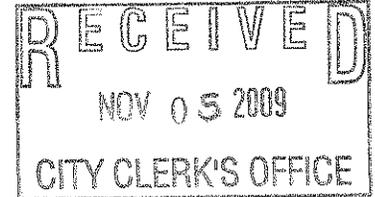
The surety bond in this case is considered a Performance Bond. A Performance Bond is a means of ensuring that all work is completed to the owner's (the City's) satisfaction. If the City's inspector or their designee has determined that the work completed by the contractor is unacceptable, and the contractor is unwilling or unable to complete the work as required, the bond is "pulled" to fund the completion of the work. The surety putting up the bond is insuring the completion of this work. In short, this is a type of insurance policy.

The bond is held by the City for at least 30 months after an excavation has been carried out, which guarantees the City will be able to repair failed patches within that time period, if the contractor is unable to do so.

The City holds a \$5,000 bond on file for each contractor pulling Excavation Permits. We do not require separate bonds for each permit a contractor pulls, however, we reserve the right to increase the bond amount (at the discretion of the Director of Public Works) based on the size of the project. Typically, a separate job-specific bond is held for work contracted by the City equal to 100% of the value of the contract.

11/9/09 Tabled

Jennie Angell  
Director, Information Services



**CITY OF MANCHESTER**  
*Information Systems Department*

November 2, 2009

Alderman Dan O'Neil, Chairman  
Committee on Administration and Information Systems  
One City Hall Plaza  
Manchester, NH 03101

Dear Alderman O'Neil;

The Information System Department, with the assistance of Finance, City Solicitor, City Auditor, Human Resources, and the Parking Division has put together the following policies and procedures so the City will be in compliance with Red Flag, State Statute and Payment Card Industry requirements.

To be in compliance with the regulations and requirements, data security policies must be in place and approved by the highest level of management.

I will have a short presentation to discuss the requirements and I am requesting that you recommend the approval of these policies.

Sincerely,

Director of Information Services

Data Security Program

November 2009

---

---

---

---

---

---

---

---

Data Security Breaches

- Major security breaches have affected millions of people worldwide
- Locally, breaches affected
  - Hannaford's Supermarkets
  - "Life is good" online marketer
  - TJ Maxx and Marshalls

---

---

---

---

---

---

---

---

Many New Regulations

- Red Flag – Identity Theft
- State Statute 359-C "Right Privacy"
- Payment Card Industry Security Standard (PCI DSS) – Credit Cards
- Health Insurance portability and Accountability (HIPPA)

---

---

---

---

---

---

---

---

## Regulation Coordination

- A committee to analyze the various regulation requirements and to coordinate the City's efforts was put together.
- This Data Security Committee has representatives from
  - Finance
  - City Solicitor
  - Risk Manager
  - City Auditor
  - Information Systems
  - Airport
  - Parking Division
  - Human Resources

---

---

---

---

---

---

---

---

## Data Security Committee

- After considerable research, the committee is making recommendations in the following areas for the Data Security Program
  - Security Policies
  - Training
  - Staffing

---

---

---

---

---

---

---

---

## Data Security Policies

- To be in compliance, formal security policies must be approved by the Board of Mayor and Aldermen.
- The following policies were drafted.
  - Network Security Policy
  - Department Network Security Policy
  - Payment Card Industry Security Policy
  - Information Technology Security Breach Incident Response Procedure

---

---

---

---

---

---

---

---

## Red Flag Requirements

- The committee is also recommending that the "Sensitive Information Policy and Program" also known as the "Red Flag Policy" be brought under this program.

---

---

---

---

---

---

---

---

## Security Policy Training

- All City Staff who have a city computer will be trained in house.
  - Security Administrators and Managers will have more in-depth training
  - Training will be conducted by Information Systems and Human Resources
  - Training must be updated at least annually
  - City staff without computers will be trained at a later date

---

---

---

---

---

---

---

---

## Training Content

- Training topics will cover
  - Network Security Policy
    - Security Administration
    - E-mail
    - E-Discovery
    - File Storage
    - Best Practices
    - Acceptable Use
  - Red Flag Policy
  - Payment Card Industry Policy (when needed)
  - Incident Response Procedures

---

---

---

---

---

---

---

---

### Without the Policies and Training

- Without the Policies and Training
  - The City would need to stop taking credit cards
  - The City would be unable to get Security and Privacy Liability Coverage
  - The City will be at greater risk for a security breach
- Information Systems would be very concerned about their ability to secure the data the City is responsible for

---

---

---

---

---

---

---

---

### Staffing

- Information Security Management has become a highly technical and specialized field.
- Compliance with the new regulations and managing the affect new technology has on data security has become an ever increasing challenge.
- A job description for a "Computer Information Security Specialist" is being development with Human Resources.
- This additional staff person will be included in Information System's 2011 budget request.

---

---

---

---

---

---

---

---

### Action Items

We are requesting the Committee on Administration and Information Systems recommend the following:

- The Security Policies be approved
- The "Red Flag" Policy be included with the other Security Policies
- Data Security Training be required for all city computer users

---

---

---

---

---

---

---

---

City of Manchester, NH  
Information Systems Department

## NETWORK SECURITY POLICY

**Background:** Network and data breaches have been occurring worldwide with increasing frequency and can enable identity and data theft. PCI, Red Flag, HIPAA and other security regulations require minimum standards of data protection. This document describes what the City of Manchester does to meet those standards. Technical adjustments to this policy will be made by the Information Systems Department when they are needed. Deviations to this policy must be approved in writing by the Director of Information Services.

- 1) Desktop Security
  - a) All PC software and hardware is purchased through the Information Systems Department or with a waiver from the Information Systems Department.
  - b) Information Systems maintains license information for all software installed on PCs.
    - i) License information is kept by fixed asset number of the CPU where the software is installed.
    - ii) Only legally licensed software is installed on City owned PCs.
  - c) Only Information Systems staff and Support Specialists authorized by Information Systems install software.
    - i) Employee owned software must be reviewed for licensing and compatibility with City applications before installation.
    - ii) Employee owned screen savers are not allowed.
- 2) Virus Software
  - a) Antivirus software that is specified by Information Systems is run on all desktops and file servers.
  - b) All PCs run real-time scanning so viruses on external storage devices will be detected.
  - c) The pattern file is updated on the main server whenever a new pattern is released from the vendor.
    - i) The pattern file is then replicated to all servers and desktops automatically.
  - d) The virus software automatically cleans and discards all viruses.
  - e) If the virus was attached to an e-mail, the recipient is notified that the attachment was dropped.
  - f) When new viruses start circulating in the world that might not be caught by the current pattern files, notification is sent to all users about what to watch for.
- 3) File Server Security
  - a) Access to File and Print servers is controlled by Windows Active Directory security.
    - i) Access to the Server Administrator passwords is limited to the highest level support personnel and only to the extent needed to provide reliable system support.

City of Manchester, NH  
Information Systems Department

- ii) Departmental file security is customized for each department at the direction of the Department Head.
  - iii) Windows passwords are required to be changed every 60 days.
  - iv) All servers have a complete backup twice monthly and a week day incremental backup at both the main and DR site.
    - (1) All non email servers have a month end backup that is stored on tape or removable disk.
- 4) Network Security
- a) All network devices that are capable, have passwords.
    - i) This includes hubs, switches, routers, jet direct boxes, DSUs, UPSs etc.
    - ii) Passwords are changed once a year or as needed.
  - b) Restricted security has been set up for some departments.
    - i) School and Police connectivity is controlled by a Firewall.
  - c) Modems are not allowed on networked PCs.
  - d) Access to the City's network from the outside is allowed via dialup with a Shiva box using dialback security. Access is also allowed using the Cisco VPN client to connect to a terminal server.
  - e) Only Information Systems personnel or those authorized by the Information Systems Department, connect devices to the network.
- 5) E-mail Security
- a) Only users authorized by their department head or his/her designee have e-mail.
  - b) E-mail can be with or without Internet e-mail capability.
  - c) All email accounts have passwords.
  - d) Users are told that e-mail files belong to the City of Manchester.
  - e) Any e-mail that is covered by FTC Red Flag rules will not be emailed without first contacting the Information Systems Department to arrange for encryption.
  - f) Only Outlook 2003 is supported for e-mail.
- 6) Internet Security
- a) Internet Access for networked PCs is only allowed from the City's Enterprise Access which goes through a proxy server and firewall.
  - b) Only users authorized by their department head or his/her designee have Internet Access.
  - c) Access to the Internet is controlled by a Proxy Server.
  - d) Access to the City's network from the Internet is protected by a firewall.
    - i) SMTP Services are allowed.
    - ii) Encrypted VPNS are allowed to terminal servers in the DMZ.
    - iii) No other external interactive connections are allowed into the City's network unless approved by the Information Systems Department.
  - e) The following standard services are allowed from the City's network out to the Internet using a Proxy server
    - i) HTTP, HTTPS, FTP
  - f) Non standard service requests are addressed on an as needed basis.
    - i) Special rules are reviewed periodically for continued need and risk assessment.

City of Manchester, NH  
Information Systems Department

- g) The Firewall cannot be remotely configured.
- 7) Application/Network Security
  - a) Application Access is reviewed annually.
  - b) Departmental Security Administrators must verify user access for each application.
    - i) Transaction, field, screen or account security within the application will also be reviewed if deemed necessary.
  - c) Requests for changes in security must be submitted and signed by a Security Administrator.
  - d) Information Systems Department holds the official list of which department has authority to grant access to which application.
- 8) Security Administrators
  - a) Each department will have one or more Security Administrators.
    - i) The Security Administrator can be the Department Head or any person or persons designated by the department head.
    - ii) The Security Administrator is authorized to request security access for users in his/her department or division.
    - iii) The Security Administrator has the responsibility of notifying Information Systems when an employee leaves the City or no longer needs the security assigned to him.
    - iv) In the event that a user needs to have a password reset, a Security Administrator for that user must authorize the resetting.
- 9) UserId/Password Security
  - a) Every user on the network has his/her own UserId/Password.
  - b) Users are not allowed to share UserIds or Passwords except for the specific situations approved by Information Systems. Authorization to share these UserIds will be provided in writing by Information Systems.
  - c) Network and Sungard /HTE passwords must be changed every 60 days.
  - d) New passwords must be unique and at least 6 characters long.
  - e) Passwords are not to be displayed or stored in obvious places.
  - f) Passwords should not be given to anyone over the telephone.
  - g) If a UserId/Password should become disabled, a Security Administrator must authorize the enabling of the UserId.
  - h) If Information Systems is informed that an employee has left the City or changed positions, the UserId will be disabled immediately pending the receipt of official information.
- 10) Outside Contractor and Guest Access
  - a) Access will be requested in advance by a security administrator.
  - b) Contractors and guests using their own equipment will only have access to the Guest/Contractor network.
  - c) Contractors and guests using City owned equipment will have their own usernames and passwords.
  - d) Contractors accessing the City's network from an external network will only have access to the City's terminal server.

City of Manchester, NH  
Information Systems Department

Reviewed 11/05/09

5-9

City of Manchester  
Departmental Network Security

Departmental Network Security Policy

Background: Network and data breaches have been occurring worldwide with increasing frequency and can enable identity and data theft. PCI, Red Flag, HIPPA and other security regulations require minimum standards of data protection. This document describes what departments in the City of Manchester must do to insure the City meets those standards. Technical adjustments to this policy will be made by the Information Systems Department when they are needed. Deviations to this policy must be approved in writing by the Director of Information Services.

- Security Administrators
  - Each department will have one or more Security Administrators.
  - The Security Administrator can be the Department Head or any person or persons designated by the department head.
  - The Security Administrator is authorized to request security access for users in his/her department or division.
  - The Security Administrator has the responsibility of notifying Information Systems when an employee leaves the City or no longer needs the security assigned to him.
  - In the event that a user needs to have a password reset, a Security Administrator for that user must authorize the resetting.
  - The Security Administrator monitors adherence to City security Policies once they are trained about these policies.
    - Application/Network Security Policy
    - Red Flag Security Policy
    - PCI Security Policy
  - A Security Administrator cannot request access for him/herself.
- UserId/Password Security
  - Every user on the City network has his/her own UserId/Password.
  - Users are not allowed to share UserIds or Passwords unless there is written authorization from Information Systems.
  - Network and Sungard (HTE) passwords must be changed every 60 days.

City of Manchester  
Departmental Network Security

- New passwords must be unique and at least 6 characters long.
- Passwords are not to be displayed or stored in obvious places.
- Users should not give anyone their password, especially over the telephone or by email. Information Systems will never ask you to do this.
- If a UserId/Password should become disabled, a Security Administrator must authorize the enabling of the UserId.
- If Information Systems is informed that an employee has left the City or changed positions, the UserId will be disabled immediately pending the receipt of official information.
- Temporary employees, contractors and guests using City owned equipment to access the City network will have their own UserIds and Passwords.
- Contractors and guests using their own equipment might have access to the Internet using the City's network. Access will depend on the level of communication equipment at the site where the access is being requested. Contact Information Systems for site specific information.
- Contractors accessing the City' network from an external network (their office) will only have access to the City's terminal server.
- Email Security
  - Only users authorized by their department head or his/her designee have email.
  - Email can be with or without Internet email capability.
  - All email accounts have passwords.
  - Any email that is covered by FTC Red Flag rules will not be emailed without first contacting the Information Systems Department to arrange for encryption.
    - Specific Red Flag items will be covered in Red Flag training and include:
      - Credit Card Information
      - Tax Identification Numbers
      - Banking Information
      - Payroll Information
      - Medical information
      - Personal Information

City of Manchester  
Departmental Network Security

- All email files belong to the City. To comply with the new e-discovery rules, new software will be installed this year that will allow easy restoration of all sent and received email.
  - Only Outlook 2003 is supported for email.
  - External email services such as GMAIL should not be used for City business because it would put the City at risk of not being able to comply with e-discovery requests.
  - Unsolicited mass emailing is not allowed except when done during a major emergency by the Emergency Operations Center.
  - Large mailing list groups with subscriber lists should be set up as Newsletters through the City's Website. The reasons for this are:
    - The recipients sign up for them without any staff involvement.
    - The newsletter manages sending large blocks of addresses without staff involvement.
      - Outlook will only send 200-250 emails per group.. Even if the email group is larger, the email system truncates the lists so not all of the desired recipients will be sent the message.
      - Trying to send bulk email via Outlook could get the City's address blacklisted. If this happens, no email from the City will be delivered.
- Application/Network Access Security
    - Application Access is reviewed annually by the Information Systems Department
      - Department Security Administrators will be asked to verify user access requirements for each application.
    - Requests for changes in security must be submitted by a Security Administrator. An email or online request from the security administrator is acceptable.
    - Information Systems Department holds the official list of which department has authority to grant access to which application.
  - Network Security
    - Only Information Systems personnel or those authorized by the Information Systems Department are allowed to connect devices to the network.

City of Manchester  
Departmental Network Security

- Modems are not allowed on networked PCs.
- User supplied wireless hubs are not allowed on the network.
- Access to the City's network from outside is allowed via dialup with a Shiva box using dialback security or using the Cisco VPN client to connect to a terminal server. Contact Information Systems for more information.
- File Security
  - User files should be stored on the network whenever possible. This is usually the S: or H: drives for internal documents and the G: drive for citywide documents.
  - Under normal conditions, user files should not be stored on local drives. These are usually C:\ or D:\ drives
  - If files need to be stored in places other than the city network, no Red Flag or PCI sensitive data can be stored in any place out of the City's control. This includes:
    - City employee home computers
    - PDAs, Cell phones and laptops
      - If storage is required on any of these devices, Information Systems must implement appropriate device security
    - Free web based file storage facilities such as Google Docs
  - Following these rules is required and is in the City's best interest because
    - Files stored on the S: and H: drives are replicated in real time off-site which protects the data from loss in the event of a disaster
    - Multiple versions of backups are available in the event of accidental deletion. Call Information Systems if you need a file restored.
    - The servers that store the documents are in a secure environment and cannot be stolen from the back seat of a car.
    - The City can comply with e-discovery requests from the court systems without taking your home computer.
    - The file storage system will not be discontinued without notice to you causing you to loose your documents.

City of Manchester, NH  
Information Systems Department

**PAYMENT CARD INDUSTRY (PCI) POLICY**

**Policy Statement:** All card processing activities and related technologies must comply with the Payment Card Industry Data Security Standard (PCI-DSS)\*in its entirety.

Card processing activities must be conducted as described herein and in accordance with the standards and procedures listed in the Related Documents section of this Policy. No activity may be conducted nor any technology employed that might obstruct compliance with any portion of the PCI-DSS.

This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. Technical adjustments to this policy will be made by the Information Systems Department.

- 1) **Scope:** This policy applies to all employees accessing customer Cardholder Data. Relevant sections of this policy apply to vendors, contractors, and business partners. Computer and network hardware will be subject to this policy if they are physically or logically on the segmented Network with Cardholder Data.
- 2) **Adherence to Standards:** Standards must be maintained for applications, employees, network components, critical servers, and wireless access points accessing Cardholder Data. Listed below are the relevant PCI DSS standards along with the City of Manchester policy relating to those standards.
  - a) **Requirement 1: Build and Maintain a Secure Network**
    - i) All external network connections and changes to the firewall and router configurations will be approved by the network manager and documented in the current work order system.
    - ii) Current network maps will be maintained for all computer Networks operated by the City of Manchester.
    - iii) Network firewalls will be deployed at each Internet connection and between any demilitarized zone (DMZ) and the Internal Network.
    - iv) Management of all Network Components will be accomplished by the City of Manchester Information Systems Department.
    - v) All services, protocols, and ports allowed through the Internet facing firewall will be documented with a business reason for the rule.
    - vi) Firewall and router rule sets will be reviewed every six months.
    - vii) All Cardholder Data will be maintained on a Network segmented from the internal City of Manchester Network with access control lists in place to allow only necessary traffic. This Network will be referred to as the Cardholder Network
    - viii) All unnecessary services will be disabled on network switches and routers.

City of Manchester, NH  
Information Systems Department

- ix) Configurations will be written to flash memory prior to disconnecting from console session.
  - x) No wireless access will be allowed on the Cardholder Network Traffic from wireless access will not be allowed on the Cardholder Network
  - xi) All necessary traffic passing through the firewall to the DMZ Network will be identified. Firewalls will be configured to only allow these protocols.
  - xii) No direct internet connections will be allowed to the City of Manchester Internal Network.
  - xiii) Connections to the DMZ Network will be documented with a business purpose.
  - xiv) No direct connections will be allowed from any external Network to the Cardholder Network.
  - xv) All Internal Network addresses will utilize NAT or PAT when connecting to external hosts.
  - xvi) No direct general internet connection will be allowed from the Cardholder Network..
  - xvii) Connections for payment card processing will be restricted to a single IP address.
  - xviii) All firewalls will be capable of stateful inspection.
  - xix) No Cardholder Data will ever be present on a DMZ Network.
  - xx) No Mobile computers will be connected to the Cardholder Network.
  - xxi) Mobile computers not owned by the City of Manchester will not be allowed on the city's Internal Network.
  - xxii) City owned mobile computers will have firewall software installed
- b) **Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters**
- i) Vendor-supplied default password and SNMP community strings will always be changed before installing any system on the Network.
  - ii) No wireless access will be permitted on the Cardholder Network.
  - iii) All wireless network access will be controlled with network access control.
  - iv) Only one primary function will be implemented per server.  
All unnecessary and insecure services and protocols will be disabled.
  - v) All routers, switches, firewalls and servers will be configured to department standards.
  - vi) All non-console administrative access will be encrypted.
- c) **Requirement 3: Protect Cardholder Data**
- i) Storage of Cardholder Data will be kept to a minimum necessary for business purposes.
  - ii) The storage duration of Cardholder Data will comply with the City of Manchester data retention policy.
  - iii) Sensitive authentication data will not be stored after authorization.
  - iv) The full contents of any track from the Credit/Debit magnetic stripe will not be stored.
  - v) The card-validation code or value will not be stored.

City of Manchester, NH  
Information Systems Department

- vi) The personal identification number (PIN) or the encrypted PIN block will not be stored.
  - vii) The PAN will be masked when displayed (the first six and last four digits are the maximum number of digits to be displayed).
  - viii) The PAN will be rendered unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs,) by using one of the following approaches.
    - One-way hashes based on Strong Cryptography
    - Truncation
    - Index tokens and pads (pads must be securely stored)
    - Strong Cryptography with associated key management processes and procedures.
  - ix) Column-level database encryption will be utilized.
  - x) Cryptographic keys used for encryption of Cardholder Data will be protected against both disclosure and misuse.
  - xi) Access to cryptographic keys restricted to the fewest number of custodians necessary. Encryption key custodians will be identified in writing.
  - xii) Cryptographic keys will be stored securely in one location on the Network with permissions that only allow authorized personnel access and one paper copy located in the password book at the information systems department office.
  - xiii) Key-management processes and procedures for cryptographic keys used for encryption of Cardholder Data, will be fully documented and implemented.
  - xiv) Generation of strong cryptographic keys must comply with PCI-DSS standards
  - xv) Encryption keys must not be transmitted as plain text. Encryption keys must only be transmitted to authorized persons.
  - xvi) Cryptographic keys will not be stored as plain text.
  - xvii) Cryptographic keys will be changed annually.
  - xviii) Old or suspected compromised cryptographic keys will be destroyed.
  - xix) Cryptographic-key custodians are required to sign a form stating that they understand and accept their key-custodian responsibilities.
- d) **Requirement 4: Encrypt transmission of Cardholder Data across open, public Networks**
- i) Strong Cryptography and security protocols, such as SSL/TLS or IPSEC, will be used to safeguard sensitive Cardholder Data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS are the Internet, wireless technologies, Global System for Mobile communications (GSM), and General Packet Radio Service (GPRS).
  - ii) Cardholder Data will not be transmitted in the unlicensed radio frequencies.
  - iii) PANs will never be transmitted by any end-user messaging technologies (for example, e-mail, instant messaging, chat).
- e) **Requirement 5: Maintain a Vulnerability Management Program**

City of Manchester, NH  
Information Systems Department

- i) Anti-virus software will be deployed on all computers and servers.
  - ii) Anti-virus will be evaluated annually to determine if it is capable of detecting and removing the latest virus and malware threats.
  - iii) Anti-virus logs will be maintained for a period of 1 year
- f) **Requirement 6: Develop and maintain secure systems and applications**
- i) All system components and software for systems with Cardholder Data will have the latest vendor-supplied security patches installed.
  - ii) Critical security patches will be installed within one month of release.
  - iii) Microsoft security notification service will be utilized for notification of critical security patches. SANS will be monitored weekly for new security vulnerability notifications. These notifications will be monitored by the Information Systems Department staff
  - iv) Router and switch configuration standards will be reviewed when new security vulnerabilities are discovered.
- g) **Requirement 7: Implement Strong Access Control Measures**
- i) Access to Cardholder Data will be restricted to employees and contracted entities. Individuals will be identified in writing who have a valid business purpose for Cardholder Data access.
  - ii) Only individuals authorized in writing will be allowed on the Network segment containing Cardholder Data. Access to the Network segment will be controlled with a network access control system.
  - iii) When accessing Cardholder Data via remote-access technologies, Cardholder Data will not be copied, moved or stored on local hard drives or removable electronic media.
- h) **Requirement 8: Assign a unique ID to each person with computer access**
- i) All users must comply with the current City of Manchester network security policy.
  - ii) Two-factor authentication is required for remote access (network-level access originating from outside the Network) to the Network by employees, administrators, and third parties utilizing Cisco IPSEC VPN with individual certificates.
  - iii) All security access requests will be processed using the City of Manchester security request system.
  - iv) Only department security administrators can request password resets.
  - v) First time passwords must be unique and changed upon first logon.
  - vi) Access for any terminated users will be immediately revoked.
  - vii) Inactive user accounts will be disabled after 90 days.
  - viii) Accounts used by vendors for remote maintenance into the Cardholder Network will be enabled only during the time period needed.
  - ix) Password procedures and policies will be reviewed by all users who have access to Cardholder Data on a yearly basis.
  - x) Group, shared, or generic accounts and passwords are prohibited except when approved by the Director of Information Services. An approved list

City of Manchester, NH  
Information Systems Department

will be maintained by the Information Systems Department and re-evaluated annually

- xvi) User passwords must be changed at least every 60 days.
  - xvii) A minimum password length of at least seven characters is required.
  - xviii) Passwords must contain both numeric and alphabetic characters.
  - xix) Changed passwords must be different from any of the last four passwords.
  - xx) Accounts will be locked out upon 6 consecutive incorrect login attempts. The lockout duration will be set to a minimum of 30 minutes or until administrator enables the user ID.
  - xxi) If a session has been idle for more than 15 minutes, the workstation will be set to lock and a password will be required to unlock the workstation.
  - xxii) Remote access connections will, by default, time out after 15 minutes of inactivity. If an extended time-out is requested, a valid business reason along with a satisfactory demonstration of system security will be required before approval will be given.
  - xxiii) A list will be maintained with all employees and contractors authorized to access Cardholder Data.
- i) **Requirement 9: Restrict physical access to Cardholder Data**
- i) All physical access to servers containing Cardholder Data will comply with the Computer room access policy.
  - ii) Video cameras will monitor any computer room housing servers that contain Cardholder Data.
  - iii) Data from video cameras will be stored for three months.
  - iv) Access to all publicly accessible network jacks will be controlled with the City network access control system.
  - v) Non City of Manchester network capable devices will not be allowed on any Internal Network.
  - vi) All network equipment will be secured in a locked room or office.
  - vii) A visitor log will be used to maintain a physical audit trail of visitor activity. The visitor log will be maintained for 3 months.
  - viii) Backup media will be stored in a secure location. No media backups that contain Cardholder Data will be stored in a non City of Manchester controlled location.
  - ix) Security for computer rooms and media storage rooms will be reviewed annually.
  - x) Any external media that contains Cardholder Data will be inventoried and its location will be tracked at all times.
  - xi) Media with Cardholder Data will be identified as confidential.
  - xii) Media containing Cardholder Data will only be handled by City of Manchester personnel.
  - xiii) Management approval is required prior to moving any and all media containing Cardholder Data from a secured area.
  - xiv) Access to storage rooms that contain Cardholder Data will be restricted to employees that have a business purpose.

City of Manchester, NH  
Information Systems Department

- xv) Backup media inventories will be conducted annually.
- xvi) Media containing Cardholder Data will be destroyed when it is no longer needed for business or legal reasons.
- j) **Requirement 10: Regularly Monitor and Test Networks**
  - i) All access to server and Network Components will be logged on a central logging server.
  - ii) All attempts to access Cardholder Data will be logged including failed attempts.
  - iii) All actions taken by users with administrative privileges will be logged.
  - iv) All access to logs files will be logged.
  - v) Logs of system components will contain the following data (if available); initialization of the audit logs, user identification, type of event, date and time, success or failure indication, origination of event, creation and deletion of system-level object, and identity or name of affected data, system component, or resource.
  - vi) System clocks and times will be synchronized to the City of Manchester Netclock.
  - vii) Audit trails will be secured so they cannot be altered. Audit trail files will be protected from unauthorized modifications.
  - viii) Viewing of audit trails is limited to designated personnel.
  - ix) Audit trail files will be backed up to a centralized log server.
  - x) Logs for external-facing technologies will be written onto a log server on the internal LAN.
  - xi) File-integrity monitoring or change-detection software will be used on logs to ensure that existing log data cannot be changed without generating alerts.
  - xii) Logs for all system components will be reviewed daily.
  - xiii) Audit trail history will be retained for one year.
- k) **Requirement 11: Regularly test security systems and processes**
  - i) The presence of rogue wireless access points will be tested for by using a wireless analyzer on a quarterly basis.
  - ii) Internal and external network vulnerability scans will be run quarterly and after any significant change in the Network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).
  - iii) External and internal penetration testing will be performed once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).
  - iv) Intrusion-detection systems will be used to monitor all traffic in the Cardholder Data Environment and be configured to alert personnel to suspected compromises.
  - v) Intrusion-detection and prevention engines will have automatic definition updates enabled if available.

City of Manchester, NH  
Information Systems Department

- vi) File-integrity monitoring software will be deployed and configured to alert personnel to unauthorized modification of critical system files, configuration files, or content files.
- l) **Requirement 12: Maintain an Information Security Policy**
  - i) The PCI security policy will be disseminated to all personnel that have the potential to encounter credit card data in their normal duties.
  - ii) Employees are required to acknowledge annually and upon hiring that they have read and understood the company's security policy and procedures.
  - iii) The PCI security policy will be reviewed once a year and updated when the environment changes or PCI DSS standards change.
  - iv) The Information Systems Department will:
    - Maintain the PCI security policy.
    - Establish, document, and distribute security incident response and escalation procedures.
    - Administer user accounts, including additions, deletions, and modifications.
    - Monitor and control all access to Cardholder Data.
  - v) A formal security awareness program will be in place to make all employees aware of the importance of Cardholder Data security.
  - vi) Policies and procedures for service providers
    - A list of service providers will be maintained by the Finance office.
    - A written agreement will be maintained that includes an acknowledgement that the service providers are responsible for the security of Cardholder Data the service providers possess.
    - Service providers will provide evidence of PCI compliance on a yearly basis.
  - vii) The incident response plan will be followed in the event of a data breach involving Cardholder Data.
    - The incident response plan will be tested yearly.
    - Employees will be trained with their appropriate responsibilities in the event of a data breach.

## GLOSSARY

**Cardholder Data:** Full magnetic stripe or the PAN plus any of the following:

- Cardholder name
- Expiration date
- Service Code

**Cardholder Network:** The segment of the City's Internal Network that contains Cardholder Data.

**DMZ:** Demilitarized zone. Network added between a private and a public Network to provide additional layer of security

**Internal Network:** Network containing servers, PC's, printers and network devices for use only by City of Manchester Personnel. This Network is segmented from the DMZ and public internet with a firewall.

**Magnetic Stripe Data (Track Data):** Data encoded in the magnetic stripe used for authorization during transactions when the card is presented. Entities must not retain full Magnetic Stripe Data subsequent to transaction authorization. Specifically, subsequent to authorization, service codes, discretionary data/ Card Validation Value/CodeCVV, and proprietary reserved values must be purged; however, account number, expiration date, and name, and service code may be extracted and retained, if needed for business.

**Network:** Two or more devices connected together to share resources utilizing common communication protocols and addressing scheme.

**Network Components:** Include, but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances

**Network Segmentation:** Isolating the Cardholder Data environment from the remainder of the corporate Network.

**PAN:** Primary Account Number is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. Also called Account Number

**Payment Cardholder Environment:** That part of the Network that possesses Cardholder Data or sensitive authentication data

**PCI:** Payment Card Industry

**SANS:** SysAdmin, assessment, Network, Security Institute (See [www.sans.org](http://www.sans.org))

City of Manchester, NH  
Information Systems Department

**Strong Cryptography:** General term to indicate cryptography that is extremely resilient to cryptanalysis. That is, given the cryptographic method (algorithm or protocol), the cryptographic key or protected data is not exposed. The strength relies on the cryptographic key used. Effective size of the key should meet the minimum key size of comparable strengths recommendations. One reference for minimum comparable strength notion is NIST Special Publication 800-57, August, 2005 (<http://csrc.nist.gov/publications/>) or others that meet the following minimum comparable key bit security:

- 80 bits for secret key based systems (for example TDES)
- 1024 bits modulus for public key algorithms based on the factorization (for example, RSA)
- 1024 bits for the discrete logarithm (for example, Diffie-Hellman) with a minimum 160 bits size of a large subgroup (for example, DSA)
- 160 bits for elliptic curve cryptography (for example, ECDSA)

Supporting Documents:

Computer Room Access Policy

Data Retention Policy

Incident Response Plan

City of Manchester, NH  
Information Systems Department

Information Technology Security Breach  
Incident Response Procedure

This document describes what an employee should do if he/she suspects there has been a security breach on the City's data network or computer systems that could compromise confidential and/or financial information. This Incident Response Plan complies with current Payment Card Industry Standards and the State of New Hampshire Statute 359-C "Right to Privacy" and will be modified as needed to maintain this compliance. The City currently does not have an Information Security Officer. Until such time as a position is created and filled, these duties will be performed by an assigned employee in the Information Systems Department.

- 1) If you suspect a security breach, as defined in the Information Privacy and Security Policy, has occurred, you should immediately:
  - a) Isolate the compromised system by unplugging its network connection cable.
  - b) Do not shut down, reboot, access or otherwise alter the machine.
  - c) Contact the Information Systems Department.
  
- 2) Upon notification of a potential security breach, the Information Security Officer ("ISO") will:
  - a) Create an incident log to document all reported facts and actions taken
  - b) Work with the individual reporting the breach to identify the systems and type of information affected
  - c) Ensure that the compromised system is properly isolated from the network and that that logs and electronic evidence are preserved on a platform suitable for analysis by a court of law
  - d) If using a wireless network, change the Service Set Identifier ("SSID") on the access point and other machines that may be using this connection (with the exception of any systems believed to be compromised).
  - e) If additional investigation is warranted, the ISO will notify the Director of the Information Systems Department who will then notify the Finance Director, the Solicitors' Office, the City Auditor, and the Mayor's Office of a possible reportable breach.
  
- 3) The Director of the Information Systems Department will designate an Information Systems Department employee to work with the ISO to investigate the situation and determine the nature and scope of the incident. Where appropriate, the ISO shall contact database and system administrators to assist in investigation efforts. Information Systems Department and the ISO shall review the entire network to identify all compromised or affected systems, including e-commerce, test, development and production

City of Manchester, NH  
Information Systems Department

environments as well as VPN, modem and third-party connections. A determination shall then be made as to the:

- a) Type of confidential information at risk (e.g., social security or credit card numbers, health information)
  - b) Number of individuals at risk
  - c) Most efficient way to bypass compromised system to ensure business continuity.
- 4) If financial account information is at risk, the investigating team must establish:
- a) Number of accounts at risk, identifying those stored and compromised on all test, development and production systems
  - b) Type of account information at risk
  - c) Account numbers
  - d) Expiration dates
  - e) Cardholder names
  - f) Cardholder addresses
  - g) CVV2
  - h) Track 1 and Track 2 data
  - i) If any data was exported and to where.
- 5) PCI forensic investigation guidelines also require investigators to establish:
- a) How the compromise occurred.
  - b) The source of the compromise.
  - c) The timeframe of the compromise.
  - d) That the compromise has been contained.
  - e) That no CVV2, Track 1 or Track 2 data is stored anywhere, whether encrypted or unencrypted.
- 6) The ISO must also perform a remote vulnerability scan of City of Manchester internet facing site(s).
- 7) After scoping the incident, the ISO will notify the Director of Information Systems Department, the Finance Director, the Solicitors Office, the City Auditor and the Mayors Office and present an overview of the situation. If the breach involves financial account information, the ISO will promptly convene the PCI Incident Response Team, including the City Auditor, Finance Department, Information Systems Department and Solicitors Office to determine if reporting is required under PCI standards or by state statute 359-C:20 *Notice of Security Breach*. Incident Response Team members should appoint delegates from within their area to serve in their capacity if they are unable to attend.
- 8) The PCI Incident Response Team will determine if a reportable incident has occurred. A reportable incident is a "suspected or confirmed loss or theft of

City of Manchester, NH  
Information Systems Department

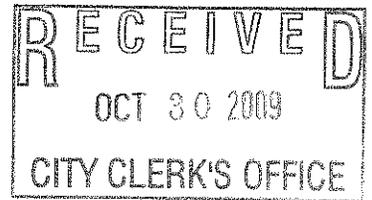
any material or records that contain cardholder data. If a reportable incident has occurred, the Incident Response Team will delegate a team member to notify the credit card companies. The contact information and specific instructions from each credit card company will be maintained by the Finance Department.

- a) Visa Fraud Control Group
  - b) MasterCard Compromised Account Team
  - c) Discover Fraud Prevention
  - d) American Express Merchant Services
  - e) Merchant bank.
  - f) Any other person defined by state statute
- 9) Follow the specific steps defined by each card company for reporting the breach.
- 10) If the credit card company, or in the case of non-financial information, the Incident Response Team, determines that the breach warrants law enforcement involvement, the PCI Incident Response Team will delegate a member of the team to notify local police and/or the FBI and Secret Service.
- 11) Individual cardholders shall be notified of the breach in accordance with the credit card company instructions and only after law enforcement determines that it will not compromise the investigation.
- 12) The Incident Response Team will draft a notification statement to be issued to those impacted by the data loss. Notification must be timely, conspicuous, and delivered in a manner that will ensure the individual receives it. Appropriate delivery methods include:
- a) U.S. Mail
  - b) Email
  - c) Substitute notice (appropriate only when individuals cannot be reached by mail or email)
    - i) Conspicuous posting of the notice on City of Manchester homepage
    - ii) Notification to major media
- 13) The PCI Incident Response Team will determine, based on the type of data compromised, the number of individuals at risk, and the general demographics of the individuals, the most effective method of notification. If notification is to be made by press release, the PCI Incident Response Team should work with the Mayor's Office.
- 14) Notification should include:
- a) A general description of the incident

City of Manchester, NH  
Information Systems Department

- b) Steps individuals can take to mitigate harm, including credit report monitoring and fraud alerts as well as sources of information designed to assist the public in protecting against identity theft;
  - c) A reminder to remain vigilant over the next 12 to 24 months; and
  - d) A customer service number that individuals can call for additional information.
- 15) As a final step, the ISO will convene the PCI Incident Response Team to review the steps the City will take to prevent future breaches and to address any deficiencies in the Incident Response Plan.

*Jane Gile*  
*Human Resources Director*



**CITY OF MANCHESTER**  
**Human Resources Department**

October 30, 2009

Alderman Dan O'Neil, Chairman  
Committee on Administration and Information Systems  
One City Hall Plaza  
Manchester, NH 03101

Dear Alderman O'Neil

On October 6, 2009, the Board of Mayor and Aldermen passed the "Sensitive Information Policy and Program" also known as the "Red Flag" policy. This program was presented to the Board because of new rules by the Federal Trade Commission. The Federal Trade Commission rules cover a limited area of need and other agencies and organizations are developing additional data security requirements. Many of those additional requirements are represented in the policies that are being presented by Information Systems Department.

The Human Resource Department is in agreement with the recommendation that the "Sensitive Information Policy and Program" be brought under the umbrella of a Data Security Program. This would help insure that the City has a cohesive approach with complying with the many new regulations for maintaining data security.

Sincerely,

  
Jane E. Gile, SPHR  
Human Resources Director

Jennie Angell  
Director, Information Services



**CITY OF MANCHESTER**  
*Information Systems Department*

CITY CLERK'S OFFICE

RECEIVED  
DEC 01 2009  
CITY CLERK'S OFFICE

December 1, 2009

Alderman Dan O'Neil, Chairman  
Committee on Administration and Information Systems  
One City Hall Plaza  
Manchester, NH 03101

Dear Alderman O'Neil,

At the last Committee on Administration and Information Systems meeting, you asked me to prepare information on how much time it will take provide all of the computer users with the necessary security training that I am requesting.

We have put together a training curriculum and have the following estimates.

Most employees will require 1½ hours of training. Each department will also have at least one person who must have Security Administrator/Manager training which will take an additional 1 hour for a total of 2½ hours of training.

This training is critical to the security of the data and systems the City is responsibility for. The incident that happened over Thanksgiving where over 400,000 emails were sent from a City account could have been avoided had there been adequate training.

I am attaching a copy of the training topics that will be covered with all users.

I am available for any questions you might have.

Sincerely,

Jennie Angell  
Director of Information Services

# User Security Training

1. Training Topics
  - a. Training Purpose
  - b. Security Administrators
  - c. User IDs
  - d. Email
  - e. Network and File Security
  - f. Red Flag Requirements
  - g. Payment Card Industry (PCI) Requirements
  - h. Security Breach Response
2. Training Purpose
  - a. Protect employees and constituents from inappropriate and/or fraudulent use of City controlled data and automated resources.
  - b. This training is required by
    - i. State Statute 359-C "Right to Privacy"
    - ii. Federal "Red Flags" requirements
    - iii. Payment Card Industry (PCI) Standards
  - a. The City needs to
    - iv. Identify Risk
    - v. Minimize Risk
    - vi. Detect Fraudulent Activity
    - vii. Respond Appropriately to Fraudulent Activity
3. Security Administrators
  - a. Each Department has at least 1 Security Administrator.
  - b. Security Administrators are designated by the department head.
  - c. Security Administrators provide Information Systems with authorization to provide network access to individuals in their department.
    - i. If you forget your password, Information Systems personnel must speak with a "Security Administrator" before they can reset your password.
  - d. Security Administrators have advanced training in the security requirements of the network and monitor the adherence of these policies in their departments.
4. UserID/Passwords
  - a. Every user on the City network has his/her own UserID/Password.
  - b. Users are not allowed to share UserIDs or Passwords unless there is written authorization from Information Systems.
  - c. Network and Sungard (HTE) passwords must be changed every 60 days.
  - d. New passwords must be unique and at least 6 characters long.
  - e. Passwords are not to be displayed or stored in obvious places.
  - f. **Users should not give anyone their password, especially over the telephone or by email.** Information Systems will never ask you to do this.

## User Security Training

- g. If a UserId/Password should become disabled, a Security Administrator must authorize the enabling of the UserId.
  - h. If Information Systems is informed that an employee has left the City or changed positions, the UserId will be disabled immediately pending the receipt of official information.
  - i. Temporary employees, contractors and guests using City owned equipment to access the City network will have their own UserIds and Passwords. Talk to your Security Administrator.
  - j. Contractors and guests using their own equipment might have access to the Internet using the City's network. Access will depend on the level of communication equipment at the site where the access is being requested. Have your Security Administrator contact Information Systems.
  - k. Contractors accessing the City' network from an external network (their office) will only have very limited access.
5. Email Security
- a. Only users authorized by their department head or his/her designee have email.
  - b. All email accounts have passwords.
  - c. **All email files belong to the City.** To comply with the new e-discovery rules, new software will be installed this year that will allow easy restoration of all sent and received email.
  - d. Sending email to Everyone\_new should only be used for city business. If you are not sure, talk to your Security Administrator or Information Systems.
  - e. City email cannot be used for political purposes or to promote personal causes (unless they are sanctioned by the Mayor's office)
  - f. Only Outlook 2003 is supported for email.
  - g. City email can be accessed from home through the Internet at [employees.manchesternh.gov](mailto:employees.manchesternh.gov).
    - i. Do not check off the "Remember my password" box.
  - h. External email services such as GMAIL should not be used for City business because it would put the City at risk of not being able to comply with e-discovery requests.
  - i. Any email that is covered by FTC Red Flag rules will not be emailed without first contacting the Information Systems Department to arrange for encryption.
    - i. Specific Red Flag items will be covered in Red Flag training and include:

## User Security Training

1. Credit Card Information
  2. Tax Identification Numbers
  3. Banking Information
  4. Payroll Information
  5. Medical information
  6. Personal Information
- j. Unsolicited mass emailing is not allowed except when done during a major emergency by the Emergency Operations Center.
- k. Large mailing list groups with subscriber lists should be set up as Newsletters through the City's Website. Contact Information Systems for help. The reasons for this are:
- i. The recipients sign up for them without any staff involvement.
  - ii. The newsletter manages sending large blocks of addresses without staff involvement.
    1. Outlook will only send 200-250 emails per group. Even if the email group is larger, the email system truncates the lists so not all of the desired recipients will be sent the message.
    2. Trying to send bulk email via Outlook could get the City's address blacklisted. If this happens, no email from the City will be delivered.
6. Network Security
- a. Only Information Systems personnel or those authorized by the Information Systems Department are allowed to connect devices to the network.
  - b. Modems are not allowed on networked PCs.
  - c. User supplied wireless hubs are not allowed on the network.
  - d. If you need access to the network from home or some other location contact Information Systems.
  - e. All Internet access is monitored and tracked.
    - i. A complete list of all sites visited by an employee can be provided to a department head if requested.
7. File Security
- a. All files stored on the network or PC belong to the City.
  - b. City equipment cannot be used for political purposes or to run a private business. Employees have been fired for this.

## User Security Training

- c. User files should be stored on the network whenever possible. This is usually the S: or H: drives for internal documents and the G: drive for citywide documents.
- d. Under normal conditions, user files should not be stored on local drives. These are usually C:\ or D:\ drives.
- e. If files need to be stored in places other than the city network, no Red Flag or PCI sensitive data can be stored in any place out of the City's control. This includes:
  - i. City employee home computers
  - ii. PDAs. Cell phones and laptops
    - 1. If storage is required on any of these devices, Information Systems must implement appropriate device security. Contact Information Systems
  - iii. Free web based file storage facilities such as Google Docs
- f. Following these rules is required and is in the City's best interest because
  - i. Files stored on the S: and H: drives are replicated in real time off-site which protects the data from loss in the event of a disaster
  - ii. Multiple versions of backups are available in the event of accidental deletion. Call Information Systems if you need a file restored.
  - iii. The servers that store the documents are in a secure environment and cannot be stolen from the back seat of a car.
  - iv. The City can comply with e-discovery requests from the court systems without taking your home computer.
  - v. The file storage system will not be discontinued without notice to you causing you to lose your documents.

### 8. Red Flags Rule

The Federal Trade Commission (FTC) put together the Red Flag Rules that require many businesses and organizations to implement a written *Identity Theft Prevention Program* designed to detect the warning signs or "red flags" of identity theft in their day-to-day operations. This protection includes customer and employee information.

- a. Red Flag sensitive information includes
  - i. Credit Card Information
    - 1. Credit Card Number
    - 2. Credit Card Expiration Data
    - 3. Credit Card Security code
    - 4. Cardholder Name
    - 5. Cardholder Address
  - ii. Tax Identification Numbers
    - 1. Social Security Number
    - 2. Business Identification Number

## User Security Training

3. Employer Identification Number
- iii. Banking
  1. Bank Routing Number
  2. Bank Account Number
- iv. Cafeteria Benefits
  1. Medical Reimbursement Information
  2. Dependent Care Reimbursement Information
- v. Medical Information
  1. Doctor names and claims
  2. Insurance claims
  3. Prescriptions
  4. Any personal medical information
- vi. Other Personal Information
  1. Date of Birth
  2. Phone Numbers
  3. Maiden Name
  4. Customer Number
- vii. Anything marked confidential
- b. Hard Copy protection
  - i. Desks and Cabinets storing sensitive information must be locked when not in use.
  - ii. Storage rooms storing sensitive information must be locked at the end of the workday.
  - iii. Desks and work areas must be cleared of sensitive information when not in use.
  - iv. Documents being distributed by the city courier should be in sealed envelopes.
  - v. Documents that are to be discarded must be either shredded immediately or placed inside a secured shred bin.
- c. Electronic Distribution
  - i. Any sensitive information that is sent either internally or externally must be encrypted and only sent to approved individuals. Contact Information Systems for assistance.
  - ii. Do not store sensitive information on local hard drives, CD/DVDs, USB drives, cell phones, PDAs, Ipods or any other mobile device unless the data is encrypted.
- d. Red Flags to watch out for include
  - i. Alerts, Notifications or Warnings from a Consumer Reporting Agency
  - ii. Suspicious documents
  - iii. Suspicious Personal Identifying Information
  - iv. Unusual use of the account
  - v. Notice of possible fraudulent activity
- e. If fraud is suspected, see your supervisor
9. Payment Card Industry (PCI)

## User Security Training

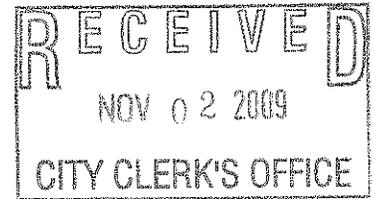
- a. PCI was set up by a consortium of Credit Card Providers including
    - i. American Express
    - ii. Discover
    - iii. Mastercard
    - iv. Visa
    - v. Others
  - b. PCI put together a comprehensive set of standards and requirements that must be met when the city takes credit cards for payments.
  - c. These standards have been set up to reduce credit card fraud.
  - d. If your department decides to take credit cards for payments over the counter, you will participate in specialized PCI training.
10. Security Breach Incident Response
- a. A Security Breach is a situation that exposes protected data to potential theft or misuse
  - b. If you suspect a security breach you should immediately:
    - i. Isolate the compromised system by unplugging its network connection cable.
    - ii. Do not shut down, reboot, access or otherwise alter the machine.
    - iii. Contact your department head or supervisor.
    - iv. Contact the Information Systems Department.
    - v. Write down everything you remember that happened.

## Sensitive Information Includes

- Credit Card Information
  - Credit Card Number
  - Credit Card Expiration Data
  - Credit Card Security code
  - Cardholder Name
  - Cardholder Address
- Tax Identification Numbers
  - Social Security Number
  - Business Identification Number
  - Employer Identification Number
- Banking
  - Bank Routing Number
  - Bank Account Number
- Cafeteria Benefits
  - Medical Reimbursement Information
  - Dependent Care Reimbursement Information
- Medical Information
  - Doctor names and claims
  - Insurance claims
  - Prescriptions
  - Any personal medical information
- Other Personal Information
  - Date of Birth
  - Phone Numbers
  - Maiden Name
  - Customer Number
- Anything marked confidential

11/9/09 Tabl

Jennie Angell  
Director, Information Services



**CITY OF MANCHESTER**  
*Information Systems Department*

November 2, 2009

Alderman Dan O'Neil, Chairman  
Committee on Administration and Information Systems  
One City Hall Plaza  
Manchester, NH 03101

Re: Credit Cards

Dear Alderman O'Neil;

The Information System Department, along with Finance, City Solicitor, City Auditor, Human Resources, the Parking Division and the Airport have been reviewing credit card acceptance for payment of city taxes and services.

We have a short presentation on the current status of acceptance and are requesting a recommendation on whether you want the City to pursue expanding the acceptance of credit/debit cards.

Sincerely,

Director of Information Services



## Credit Cards

### Credit Card Acceptance In Manchester

November 2009

---

---

---

---

---

---

---

---



## Current Situation

- Many departments have expressed the desire to accept credit cards for payment. This would
  - offer convenience to constituents
  - reduce the amount of cash in City departments
  - standardize cash receipting in many departments
  
- This is the standard way to do business in the commercial world.

---

---

---

---

---

---

---

---



## Current Situation

Credit Cards are taken at

- Victory parking garage
- City parking kiosks
  - 40% of revenue is paid with credit cards
- Derryfield Country Club
- Airport parking garage
  - 78% of revenue (\$16 million) is paid with credit cards
- Online payments on the City's website -
  - over \$670,000 in first 4 months of this fiscal year
    - Parking Tickets      Property Taxes
    - Water Bills          Sewer Bills
    - Motor Vehicle Registrations

---

---

---

---

---

---

---

---



### Credit Cards Analysis

- A committee to analyze credit card options, requirements, and costs was created. The committee consists of representatives from
  - Finance
  - City Solicitor
  - Risk Manager
  - City Auditor
  - Information Systems
  - Airport
  - Parking Division
  - Human Resources

---

---

---

---

---

---

---

---

---

---



### Credit Card Data Loss in the News

- Owners of T.J Maxx, Marshalls and Bob's Stores compromised. That breach affected more than 94 million credit and debit card accounts.
- Data thieves broke into computers at supermarket chains Hannaford Brothers and Sweetbay, stealing an estimated 4.2 million credit and debit card numbers.
- Boston clothing retailer Life is Good had nearly 10,000 credit card numbers stolen from the company's database.

---

---

---

---

---

---

---

---

---

---



### Payment Card Industry

- In response to several high profile data breaches, Payment Card Industry (PCI ) standards changed in October 2008.
- PCI Data Security Standard (PCI DSS) is a set of comprehensive requirements for enhancing Credit Card data security.
- Payment Card Industry Security Standards Council was founded by American Express, Discover Financial Services, MasterCard Worldwide, Visa International and others.
- Compliance with the PCI standards is required by the Payment Card Industry of all merchants accepting credit cards.

---

---

---

---

---

---

---

---

---

---



### Current Situation

- For the City to continue to allow credit card payments in the parking garages and at the parking kiosks, the required security improvements are being put into place.
- These improvements include
  - Written policies
  - Software and hardware upgrades
  - Annual testing by an outside company
  - Annual data security training
- Airport and Parking Division are paying for any required upgrades out of their 2010 budgets.

---

---

---

---

---

---

---

---



### Risks of Noncompliance

- Fines from the Credit card processor.
  - These fines are directly from Visa, MasterCard etc.
- Restrictions on Credit card acceptance.
- Permanently prohibited from accepting Credit cards.
- Increased risk of a data security breach

---

---

---

---

---

---

---

---



### Impact of Loss of Credit Cards

- Victory Garage would need an additional cashier
- Airport would lose its revenue base
- Parking kiosks would lose their effectiveness
- Constituents would lose the convenience of online services

---

---

---

---

---

---

---

---



## Benefits of Compliance

- City will not be in violation of the contracts they executed.
- Visa and MasterCard may waive fines in the event of a breach.
- Improves overall security and helps compliance with other data protection standards (Red Flag, State Statutes, etc).
- Reduced exposure to hacker activity. Hackers typically target the easiest opportunities.
- Reduced liability insurance costs.

---

---

---

---

---

---

---

---



## City Potential Liability

- If a data breach is suspected
  - An approved external data security company must examine the suspected compromised systems.
  - This cost would be the City's responsibility. (\$10,000-\$20,000)
- If a breach is verified, fines will be assessed by the Credit Card issuers within 3-5 months. Fines from MasterCard in the Heartland data breach exceeded \$6 million. If the City is compliant with the PCI standards, these fees may be waived.
- The City could be liable for all fraudulent charges on the compromised credit cards.

---

---

---

---

---

---

---

---



## PCI Data Security Compliance for Manchester

- Requirements to maintain existing credit card acceptance
  - Approval and implementation of the new Security Policies.
  - Procurement of security software and hardware required by PCI DSS.
  - Performance of quarterly security audits.
  - Implementation of physical security requirements for PCI DSS.
  - Implementation of training program
- Airport and Parking are paying for their requirements

---

---

---

---

---

---

---

---



### Expansion of Credit Card Acceptance to Other Departments

- City needs to issue an RFP for Credit Card services
- Proposals would specify what security services the vendor will provide
- The City will then be able to estimate any additional costs
- Additional costs will include staff training
- The City will need a Computer Information Security Specialist position
  - This position would be partially allocated to the enterprises

---

---

---

---

---

---

---

---



### Should the City Take Credit Cards in More Places?

- Credit Cards will
  - reduce the amount of cash in offices
    - Reduces robbery exposure
    - Reduces cash shrinkage exposure
  - reduce the amount of time required for counting, balancing and creating deposits
  - reduces cash handling errors
- Your constituents are asking for it
- This is how business is conducted today.

---

---

---

---

---

---

---

---



### Next Step

- If the Board directs us to pursue the expansion of credit card acceptance
  - A plan will be developed for each department to comply with all of the necessary standards
    - Departments must be in compliance before they start accepting credit cards
    - Cost items will be included in the 2011 budget request

---

---

---

---

---

---

---

---



### Next Step

- Finance will prepare the RFP for citywide credit card services.
- We will come back to the Board with the various options and recommendations on how to proceed.

---

---

---

---

---

---

---

---



### Action Items

Should we proceed with the expansion of credit card acceptance?

---

---

---

---

---

---

---

---



Matthew Normand  
Acting City Clerk

**CITY OF MANCHESTER**  
*Office of the City Clerk*

**MEMORANDUM**

TO: Committee on Administration/Information Systems  
Aldermen O'Neil, Garrity, Osborne, Pinard, Murphy

FROM: Matthew Normand  
Acting City Clerk

DATE: February 6, 2009

RE: Proposed Policy on Street Closures

On November 24, 2008, the Committee requested that the City Clerk's Office review the current procedures for street closure for special entertainment events and propose some suggestions to improve the process. After some prior discussions with the Parking Division, Police, and Mayor's Office as well as members of the Committee, we have attached some recommendations for the Committee's consideration.

Our intent is to continue permitting street closures for entertainment related events under current procedures and ordinances but to add some additional oversight by including the Parking Division approval, notification to abutting businesses, and Committee on Administration involvement under certain conditions.

Please call me should you have any questions or concerns. Thank you.

pc: Sgt. J. Flanagan, Police Department  
T. Clark, Solicitor's Office  
B. Stanley, Parking Division  
S. Thomas, Mayor's Office

## Proposed procedures for street closures for entertainment purposes

### Policy

Temporary street closures for Entertainment Place of Assembly Permits may be granted by the City of Manchester based on the following standards:

1. Application for street closure must be submitted at least 30 days prior to event.
2. Any application received after deadline shall be denied by the Office of the City Clerk and submitted to Committee on Administration/Information Systems for approval.
3. The activity may not impair normal Fire and Police operations.
4. The City shall not incur additional costs related to street closure.
5. Businesses directly abutting the proposed street closure will be notified by Office of the City Clerk.
6. Multiple requests for street closures on same block in a close proximity of time may be referred to the Administration/Information Systems for consideration.

### Procedure

1. Application must be filed with the Office of the City Clerk with appropriate approvals from Police, Fire, Highway and the Parking Division.
2. Applicant must provide detailed plans for street closure with application. Details shall include times and date of closure, description of event and purpose for request.
3. Office of City Clerk will notify in writing all abutters affected by closure.
4. All clean-up is responsibility of applicant.
5. Any additional costs for City services shall remain the responsibility of applicant.
6. All decisions of the Committee on Administration/Information Systems are final.

Tabled 3/16/09

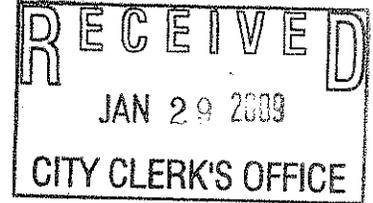
Thomas R. Clark  
City Solicitor



Peter R. Chiesa  
Gregory T. Muller  
John G. Blanchard  
Jeremy A. Harmon

Thomas I. Arnold, III  
Deputy City Solicitor

**CITY OF MANCHESTER**  
*Office of the City Solicitor*



January 29, 2009

Matthew Normand, Acting City Clerk  
City of Manchester  
One City Hall Plaza  
Manchester, NH 03101

RE: **Naming Rights Policy**

Dear Matt:

Enclosed is the draft naming rights policy requested by the Board at its meeting on December 16, 2008.

Very truly yours,

Thomas R. Clark  
City Solicitor

TRC/hr  
Enclosure

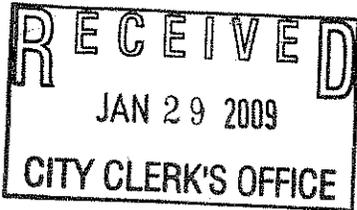
In board of Mayor and Aldermen

Date: 2/3/09 On Motion of Ald. Lopez

Second by Ald. Sullivan

Voted to refer to Committee on Administration

  
City Clerk



DRAFT

POLICY ON NAMING  
CITY PROPERTY

All requests to name city owned or controlled real property, buildings or structures shall be submitted, in writing, to the Board of Mayor and Aldermen for referral to the department or entity having jurisdiction over the real property, building or structure. The written request shall contain the following information:

- Background information detailing the appropriateness of the intended name.
- Background information on the real property, building or structure in question.
- How any costs associated with the naming shall be funded.

The department or other entity shall review the written request and forward a recommendation to the Board of Mayor and Aldermen for referral to the Committee on Lands and Buildings.

The Committee on Land and Buildings shall take such action as it deems appropriate and report its recommendation to the Board of Mayor and Aldermen.

**To the Board of Mayor and Aldermen of the City of Manchester:**

The Committee on Public Safety, Health and Traffic respectfully recommends, after due and careful consideration, that the request from Barbara Potvin, New England Sampler, for the City to hold a public forum to discuss the closing off of city streets be referred to the Committee on Administration/Information Systems.

*(Unanimous vote)*

Respectfully submitted,

  
Clerk of Committee

At a meeting of the Board of Mayor and Aldermen held October 21, 2008, on a motion of Alderman Sullivan duly seconded by Alderman O'Neil the report of the Committee was accepted and the recommendations adopted.

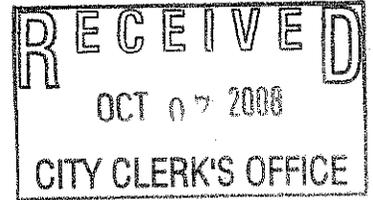
  
Deputy City Clerk



The  
New England  
Sampler

Specializing in  
New England Products  
&  
Specialty Foods

42 Hanover St.  
Manchester, NH 03101  
603.626.4477



September 26, 2008

Dear Mayor Guinta, Aldermen Mark Roy, Mike Lopez, Dan O'Neil, Peter Sullivan & Brandy Stanley,

As you may already know, the Palace Theatre held a fundraising event last Thursday, September 18<sup>th</sup>. Attached is a petition signed by a number of business owners and managers located on the one-way section of Hanover St., between Chestnut and Elm Street. Peter Ramsey, the Executive Director of the Palace Theatre has been provided a copy of this petition and discussions have been held with Peter. Stephanie Lewry, from Intown was present at a discussion between Peter Ramsey, and myself, Barbara Potvin regarding this petition, the blocking off of the street and the implications of blocking the streets off for any such event.

During this discussion, Peter Ramsey had suggested that the City of Manchester might consider holding a Public Forum to discuss the process of closing off city streets and the impact that these closings have on local small businesses as well as the benefits drawn by the City of Manchester and its local citizens. After great consideration and input from other businesses on Elm St., that have faced this situation and dilemma, I agree with Peter that a public discussion would be helpful and could provide us all, including the City Hall with a policy that addresses and considers the welfare of all business owners/managers, local community members as well as Manchester City Hall.

Feel free to contact me at 603-626-4477 with any questions you might have regarding this request and this petition.

Sincerely,

Barbara J. Potvin

Owner

The New England Sampler

cc: Peter Ramsey, Stephanie Lewry

September 19, 2008

We the signed business managers and owners would like the City of Manchester to know of our discontent and concern regarding the blocking off of Hanover St., between Chestnut and Elm on Thursday, September 18, 2008 for the Palace Theatre's Wine Tasting and Fundraising event. It is our understanding that they did not have permission to block off the parking spaces, but did have permission to block the street after 2PM. However, it should be noted, that most business owners and managers were not included in this decision nor were the majority notified that this would occur prior to this week. Many were never informed and only realized on Thursday when they saw the cones along the parking space.

Further, our concerns include:

- Most businesses were not informed that the streets and parking spaces along this stretch of Hanover St. would be inaccessible throughout most of the day.
- As business owners and managers we are concerned with the significant loss of revenue for each business located on this section of Hanover St. Many businesses had to either reschedule or cancel appointments. Others noted a drop in their sales because of the inaccessibility of the street and on-street parking. Some even ended up closing early due to the loss of revenue and lack of access for customers.
- Our concerns also include loss of revenue for the City of Manchester. Many parking spaces on both sides of the road were blocked off as early as 8AM.
- Finally, there is a concern for public safety and property, whenever such events occur, since ambulances and fire trucks can not safely access Hanover St. between Chestnut and Elm during the aforementioned events.

The following business owners/managers would like register their concerns regarding the lack of opportunity to give input and recommendations, as well as the lack of appropriate notification as to when these types of events will be occurring.

Name:	Business Name:	Address:
Scott Seward	Suddenly Swans Gourmet Del.	87 Hanover
Samina J. Delaski	Al Bazaar Lim. Corp	81 Hanover St
Bill Miller	OK Parkers S.	89 Hanover St
Jim Kappeler	Ribent Photographers	72 HANOVER ST
Chris Aker	EMBASI	54 Hanover
Anchea Lessard	Shop Estella	52 Hanover St.
Jeanine Sylvester	Runners Man	36 Hanover st
Susan Maria	Stony (B) Auctioneers	32 HANOVER ST
Sun Chung	Korean Place Restaurant	110 Hanover St.
Zoe Huel	Cottages Design Furniture	73 Hanover St.
Barbara Winton	The New England Sampler	42 Hanover St
Janice	Jetton Hanover	26 Hanover St.
John Bulm	Soly Luna Jewelry	83 Hanover St