



Pedro E. Segarra
Mayor

EXECUTIVE ORDER

EO Number: 15-1

Topic: Cybersecurity

Effective Date: January 15, 2015

WHEREAS, Responsibility for the health, safety, and welfare of Hartford residents is of paramount importance to City government, and

WHEREAS, City government increasingly relies on local and global computer networks and its own electronic infrastructure to provide services for our community, and

WHEREAS, The City must be able to defend against, and quickly recover from, any disturbance to its electronic infrastructure, whether resulting from accidental or intentional, natural or human-caused disaster, and

WHEREAS, One aspect of the City's strategy for reducing the risk of disturbance is to make our electronic systems and infrastructure more resistant to penetration, and

WHEREAS, In order to maintain the City's cybersecurity, collaboration between and among City departments, MetroHartford Information Services (MHIS), and other levels of government is essential,

NOW, THEREFORE, BE IT PROMULGATED BY EXECUTIVE ORDER OF THE HONORABLE PEDRO E. SEGARRA, MAYOR OF THE CITY OF HARTFORD:

That Hartford City Government, including all City departments, agencies, divisions, bureaus, boards, and commissions, shall implement the following instructions and all business partners, contractors, vendors, and consultants shall also be bound by this Order while conducting business with the City of Hartford.

Cyber Intrusion Command Center

There shall be established a collaborative effort known as the Cyber Intrusion Command Center (“CICC”), which shall be chaired by the Office of the Mayor and shall consist of all City departments. The CICC shall receive assistance from the Federal Bureau of Investigation (“FBI”), the United States Secret Service, and any other appropriate federal or state agency. The cybersecurity goals of the CICC are:

- To facilitate the identification and investigation of cyber threats and intrusions against City assets,
- To ensure that incidents are quickly, properly, and thoroughly investigated by the appropriate law enforcement agency,
- To facilitate dissemination of cybersecurity alerts and information,
- To provide a uniform governance structure accountable to City leadership,
- To coordinate incident response and remediation across the city,
- To serve as an advisory body to City departments,
- To sponsor independent security assessments to reduce security risks, and
- To ensure awareness of best practices.

All departments must contribute personnel, resources, and data to the Cyber Intrusion Command Center in order for it to succeed. The nature and extent of each department’s involvement will depend on the nature and extent of their cyber assets, with those deemed to have the most critical assets being more heavily involved in this collaborative effort. It is not acceptable for any City department to withhold information from the CICC regarding cybersecurity issues. In addition, every department will:

- Establish and maintain permanent liaisons with the CICC,
- Report information about significant cyber-related events occurring in the department,
- Identify personnel who require notification of threats, and
- Provide resources for cooperative actions as situations may require.

Members of the CICC will report to the Mayor and Council, as directed by those offices, regarding the issues being addressed by the group. The existence of this collaborative effort does not eliminate the need for departments to perform actions required of them by law and/or regulation. Further, this order is not intended to supersede, replace, or interfere with the applicability of all relevant federal, state, and local laws relating to privacy and the confidentiality of personal information.

Within 10 days of the date of this Executive Order, the Office of the Mayor will organize a working group of key City departments that will propose a more detailed organizational structure for the Cyber Intrusion Command Center. The working group will present the proposed structure to the Office of the Mayor for approval within 30 days of this Order.

City Department Responsibilities

In addition to participating in the Cyber Intrusion Command Center, each department must enhance its own cybersecurity. Each department plays a unique role in securing its departmental information and personal data of its users, and Hartford residents. Each department is responsible for usage of the City network by its employees and contractors. All City departments should review and comply with the related citywide policies. The policies may be found on the City intranet at:

<http://citynet.hartford.gov/AdministrativePolicies/AdministrativePolicies.aspx>

Departments are responsible for keeping up-to-date with all City cybersecurity policies. Furthermore, departments are encouraged to present their recommendations for new cyber policies to the Chief Information Officer of MHIS.

All departments must adhere to the following minimum standards.

Prevention of Unauthorized Access: Limiting data and network access to authorized individuals is a primary means for securing the City's information technology assets. Departments must take the following actions.

- Limit physical, wireless, and remote access to City workstations, systems, networks, and email to authorized City employees and contractors.
- Deactivate all passwords and network access for employees who have left City service.
- Deactivate all access for employees who have not accessed their network within the past 60 days, unless the employee is on a medical leave or other authorized leave approved by a manager or department head.
- Implement physical security measures for City computers, servers, and network ports to physically separate them from unauthorized users. This may include moving them behind locked doors and/or into restricted areas.
- Include security restrictions in computer kiosks dedicated to public usage to ensure that they are logically separated from City networks and data.
- Abide by the IT Resources Policy for Wi-Fi network access and services.

Promotion and Enforcement of Password Security: All systems, networks, e-mail, and screensavers must be password protected. This includes all departmental applications and network drives that contain sensitive, personal, or confidential information. In addition, departments must:

- Set password protected screensavers to activate after 15 minutes of workstation inactivity.
- Assure that passwords meet the City's minimum password requirements and are changed every 90 days.
- Inform all employees that passwords shall contain a combination of upper and lower case letters, with numbers and symbols, so that they are considered to be "strong" passwords.

- Use passwords on all devices that are used for City business, including hand held devices such as smart phones, tablets etc.

Maintenance of Anti-Virus Software: Servers, laptops, desktops, and other devices must have anti-virus software installed and updated at all times. Departments must ensure that anti-virus software is installed at every workstation and virus definitions are updated periodically.

Promotion of a Culture of Cybersecurity Awareness: Departments must periodically remind their employees and contractors of City cybersecurity policies and best practices. Furthermore, cybersecurity considerations shall be incorporated into all new department systems or projects when applicable.

Planning for Business Continuity and Disaster Recovery: Departments must assess their mission critical systems and plan for both continuity of operations and disaster recovery in the event of a successful cyber-attack. Each department shall create, and update annually, a Continuity of Operations Plan (COOP), which should include a listing of mission critical systems and planned responses in the event of a cyber-attack. Additionally, each department shall establish a data backup process for mission critical systems to allow system restoration without the loss of significant data.

City Employee and Contractor Responsibilities

City employees are our first line of defense in ensuring that City systems are protected from intruders. Employees are in the best position to protect systems and to report problems at an early stage, before an issue impacts the City more broadly. All City employees are encouraged to promote a culture of cybersecurity within their departments and to report issues that they identify. It is also incumbent upon City employees to act ethically and with integrity when using and accessing the City's computer systems. Additionally, employees have a responsibility to protect these systems from disruption, intrusion, or attack. With these principles in mind, employees should engage in the following practices.

Prevention of Unauthorized Access: Limiting data and network access to authorized individuals is a primary means for securing the City's IT assets. City employees have a responsibility to ensure that all City IT assets are protected and that only authorized individuals have access to these important City assets.

Promotion of Password Security: Every employee's user ID and password provides critical protection from unauthorized cyber-attacks. Employees shall not share this information with anyone else, including other City employees. Employees should:

- Set their computers to automatically require password protected screensavers after 15 minutes of workstation inactivity.
- Change their passwords every 90 days.
- Use passwords that contain a combination of upper and lower case letters, with numbers and symbols, so that they are considered to be "strong" passwords (please

refer to the Acceptable Use Policy for IT Resources #011 for further details on the minimum password requirements that must be followed).

- Use passwords on all devices that are used for City business, including hand held devices such as smart phones, tablets, etc.

“Smart” Usage of Internet and E-mail Attachments: Internet usage and e-mail are primary methods used to install malicious software onto computers and networks. Employees and contractors must practice vigilance in the usage of the Internet and e-mail (please see the IT Resource and Mobile Device Policies). Practices that should be employed include the following.

- Never enter personal or sensitive City information into untrusted websites.
- Delete e-mails and e-mail attachments from unrecognized sources.
- Never download material from untrusted sources.
- Maintain Internet browser security settings of medium or higher.
- Trust your instincts. If an email or email attachment seems suspicious, don't open it, even if your anti-virus software indicates that the message is clean. At the very least, contact the person who supposedly sent the message to make sure it's legitimate before you open the attachment. However, especially in the case of forwards, even messages sent by a legitimate sender might contain a virus. If something about the email or the attachment makes you uncomfortable, there may be a good reason. Don't let your curiosity put your City computer at risk.
- Be cautious when visiting web links or opening attachments from unknown senders.
- While on the Internet, do not click on any links within pop-up windows.
- Don't follow email links claiming to offer anti-spyware software.
- Use caution when downloading free downloadable software. Do not download programs from sites you don't trust; you should realize that you may be exposing the City's computer to spyware by downloading some of these programs.

No Usage of Unauthorized Devices: Cyber attackers are looking for “points of entry” into the City network or a department's systems. Practices that should be employed to prevent entry include the following.

- Employees should not connect personal or unauthorized devices into their work computer. Such devices include flash/USB drives, external drives, music devices, smart phones, untrusted CDs or DVDs, or other similar devices.
- Home and work devices should be kept separate. Employees should not use the same flash drives for home and work.
- Employees should avoid copying sensitive City data onto a USB device.
- Bluetooth on City devices shall be disabled when you are not using it, in order to prevent unauthorized access.

Usage of Systems Solely For City Business Activities: Employees shall not use computers for non-business related access to audio and/or video internet sites to listen to music or watch video clips. The network traffic created by accessing these audio and

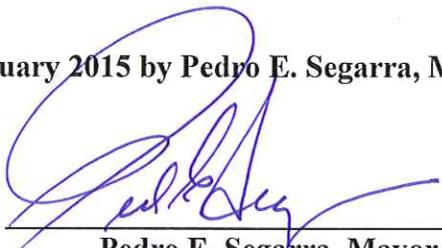
video sites places an enormous burden on the City's networks, negatively affecting the ability of other employees to access the internet for legitimate business activities.

Responsibilities of MetroHartford Information Services (MHIS)

The City's information technology department, MHIS, as the unifying technology department throughout the City, will be a key player in ensuring the success of our City's technology security strategy. MHIS is responsible for all firewalls, intrusion detection systems, application control engines, annual security audits and penetration tests, and is also responsible for validating, to the Cyber Intrusion Command Center, that departments are diligent in their security practices. Therefore, MHIS shall ensure that:

- All cyber technology policies are up to date and easily accessible to all City employees for use and reference,
- All City employees receive annual training on cybersecurity,
- All software is maintained, including updates and patches, as recommended by the manufacturer, and
- All City departments have proper technology to ensure that they can comply with this Order. This shall include, but not be limited to
 - Developing mechanisms to determine whether dormant e-mail accounts have been deactivated,
 - Providing all departments with the technology or software needed to automatically prompt employees to change and update passwords every 90 days, and
 - Equipping all City computers with password protected screensavers that will activate after 15 minutes of workstation inactivity.

Signed this 15th day of January 2015 by Pedro E. Segarra, Mayor of the City of Hartford.



Pedro E. Segarra, Mayor