



NEW YORK CITY

Office of Emergency Management

**NYContinuity**

*Emergency Management Newsletter for Businesses*

NYC OEM

December 2009

Welcome to **NYContinuity**, a monthly publication to help you prepare for emergencies, strengthen your continuity plans, update you on emergency management news, and inform you about events and resources available to businesses in New York City.

This month's issue focuses on technology. Information security is essential to business. The Small Business Corner describes actions businesses can take to protect their data from malicious attacks and hardware failures. This month's "Flu Feature," part of **NYContinuity's** continuing efforts to support flu planning, discusses best practices for telecommuting.

This issue also announces a special event: the Department of Homeland Security is hosting a public meeting regarding the Private Sector Preparedness Certification and Accreditation (PS-Prep) program. Read on to find out how you can get involved.

**NYContinuity** is a newsletter for small business owners and continuity professionals brought to you by OEM.

## Small Business Corner: **Information Security and Recovery**



### **Small Business Information Security: The Fundamentals**

Customers and employees trust your business with important personal and financial information. If this information is lost or compromised, it could be a blow not only to your business, but also to your client base and support network.

To help small business owners protect information, the [National Institute of Technology and Standards \(NIST\)](#) released *Small Business Information Security: The Fundamentals*, a brief guidebook small business owners can use to secure their data.

The guidebook outlines necessary actions like installing and updating anti-virus and anti-spyware software and installing firewalls to prevent phishing (theft of personal information) and malicious attacks through the internet. NIST also highly recommends precautions such as opening only secure e-mail attachments and banking only over secure connections, to make sure that you are only dealing with people you trust. The guidebook suggests putting your information policies in writing and discussing them with employees to ensure their compliance.

[Read more about how to secure your business's information](#) or [watch a video](#) that accompanies the NIST guidebook.

### **Information Recovery**

One of the most important steps in securing your information can also be one of the easiest. Regularly backing up your computer can help you recover from a physical or technological emergency. Certain software programs can be set to back up contents automatically, and you can use a CD or flash drive to store records off-site in a safe location. Make sure you test back-up copies: you do not want to discover after an emergency that you are unable to access your information.

If you do suffer a loss of data from a hard drive failure and find yourself without a back-up, there are companies that specialize in data recovery that may be able to help. The New York State Archives maintains a [list of data recovery vendors](#).

## Flu Feature: **Telecommuting Best Practices**



Many pandemic plans encourage employees to work from home as a means of reducing person-to-person contact. If telecommuting is part of your plan, do you know that your employees can successfully work from home? If possible, have employees practice telecommuting, so that they can solve any problems that might come up before an emergency occurs. Consider having multiple employees log on to your network remotely at the same time to test if it can handle the increased traffic.

The Department of Homeland Security studied a pandemic's potential impact on telecommunications networks in 2007 and generated a series of recommendations to encourage successful telecommuting.

[Read DHS's best practices for networks and telecommuters during a pandemic](#) (see Appendix C, page 43).

## Upcoming Event: **Public Meeting to Discuss Private Sector Preparedness Standards**



**Homeland Security**

The Department of Homeland Security (DHS) will hold a public meeting on December 10, 2009 at the LaGuardia Marriott to discuss the Private Sector Preparedness Accreditation and Certification (or PS-Prep) program. The meeting will provide a forum for discussion of the standards that DHS has selected.

A result of the 9/11 Commission's recommendations, the PS-Prep program will enhance nationwide resilience by encouraging private sector preparedness. The program will certify organizations that have voluntarily conformed to DHS's preparedness standards.

**When:** December 10, 2009, 1 PM - 5 PM

**Where:** LaGuardia Marriott, 102-05 Ditmars Boulevard, East Elmhurst, NY 11369

[Learn more about the meeting and the PS-Prep program.](#)

If you have any topics or themes that you would like to see covered or any suggestions for how we may improve this newsletter, please send an e-mail to [publicprivate@oem.nyc.gov](mailto:publicprivate@oem.nyc.gov). To see if your topic has been covered in a past issue, please visit the [NYContinuity Archive](#).

Sincerely,  
The **NYContinuity** Team

*The NYContinuity newsletter is being offered for general informational purposes only. Under the circumstances, the City assumes no duties to registrants or others and disclaims any right for such persons to rely on the newsletter or its messages.*

Not a member? [Click here](#) to subscribe for NYContinuity!

Email Marketing by

