35870

Exhibit A

COMPUTER VIRUS PREVENTION AND RECOVERY

March 8, 2000

Computer Virus Prevention and Recovery

Mission Statement

The Virus Prevention and Recovery Plan (Plan) is designed to provide maximum security while minimizing loss-of-service. The goal is to minimize damage to the City's Information Technology resources and services, while simultaneously keeping these resources and services available.

1 Introduction

This document is intended to provide a clearly defined, citywide approach to computer virus prevention and protection as well as post-detection recovery. It is a living document that will grow as the City gains experience with new kinds of threats.

The plan includes five components: identification, isolation and notification, eradication, and service restoration and debrief. It employs a systematic escalation of activities based on the seriousness of the contamination. At the same time, it is understood that the components will frequently occur as parallel activities. Providing a new twist on the phrase 'speed kills', speed of response is the corporate terrorist's deadly enemy. The need for rapid, organized response places an extremely high level of importance on all communication aspects of the Plan.

2 Tactical Plan

The Tactical Plan is designed to escalate systematically from initial identification, through risk analysis, proper virus isolation and notification, and eradication procedures. However as previously stated, activities may occur in parallel to expedite overall response.

2.1 Phase I: Initial Rapid Identification

Phase I: Initial Rapid Identification is carried out as soon as a virus is detected. It includes a quick, systematic analysis and culminates with notification of the Rapid Response Team (see Phase I, Notification component below). Identification can occur in three ways.

2.1.1 Identification

- Automated notification from virus protection vendor or monitoring
- External notification from business partners and/or IT community
- Internal discovery

2.1.2 Initial Research / Triage

- Determine the type and extent of virus.
- Initiate isolation by bureau to the extent possible (depends on staff availability and manner of initial discovery

2.1.3 Immediate Notification

The following notification procedures are applicable for all virus infections, no matter how localized.

- During normal business hours, contact the BIT Help Desk (823-5199)
- After normal business hours, weekends and holidays, contact BIT Operations (823-6922)
- Incident Commander (Bureau of Information Technology Director or designee)
- Rapid Response Team (three member, multi-bureau virus testing team, selected from APPENDIX A by Incident Commander - or - from pre-established, rotational, on-call teams)
- Lead Communications Individual

2.2 Phase II: Isolation and Citywide Customer Notification

2.2.1 Isolation

- Based on the initial risk assessment (extent of contamination, time of day, day of week), the Incident Commander will authorize isolation measures to minimize further contamination/recontamination (from external sources and/or between all or selected City E-mail subsystems). These actions may include one or all of the following:
    - Temporary shut down of all or selected E-mail services.
    - Temporary shut down of Internet services.
    - Temporary shut down of connections to the backbone network.
    - Temporary shut down of the backbone network.

2.2.2 Continued Research and Testing

- If discovered locally, move a copy of the virus to the 'Clean Site[1]'.
- If informed by vendor, download a copy of the virus to the 'Clean Site'.
- Research what is known externally (CERT, virus protection vendors, others).
- Maintain contact with viral news sources including anti-virus vendors and Web sites (www.nips.gov, www.nai.com, www.symantec.com, www.mcafee.com, www.avertlqavs.com, www.cert.org, www.city/bit/virus.htm).

[1] If funded via the OF&A FY 2000 unmet business needs request, the Clean Site establishes a quarantined environment within which virus research is conducted. Multiple private, dedicated, conventional telephone (POTS) lines should serve the Clean Site. The environment will include servers and workstations representative of those deployed across the City. It will house and safeguard fundamental software necessary to restart computer systems in response to events ranging from viral contamination to catastrophic disasters.

- Determine how the virus feeds (host software) and replicates (user-dependent, time sensitive, etc.). Determine the viral effects (e.g. nuisance versus destructive). Continually update the risk assessment.
- Continually verify that anti-virus tool distribution proceeds effectively.
- Determine point-of-entry and contamination path, review pertinent log files and diagnostic procedures.
- Estimate initial damage report.
- Determine 'Emergency Status' (Incident Commander).

2.2.3 Notification

The *Phase II Notification* component includes options that will be exercised according to the seriousness of the event and the previously taken isolation steps. Note that during the *Phase II: Notification* component, caution must be exercised to create the appropriate level of awareness...NO FALSE ALARMS.

- Notify Mayor. Recommend IT Emergency Status. Mayor declares an IT Emergency and Level if required. Notify Emergency Operations Center if appropriate.
- Establish and distribute Budget Control Number for financial and statistical tracking (Incident Commander).
- Establish and support bi-directional, ongoing communication with customers and business partners.
- Notify appropriate E-mail administrators, IT Managers.
- Notify Public Information Officers as appropriate.
- Develop initial 'citywide' statement to employees (Voice Mail, Intranet, elevator fliers, etc.).
- Develop initial press release.
- Notify business partners and media.
- Notify IT internal and external partners (BIT Help Desk and administrative personnel, enterprise applications that may be affected, emergency response bureau managers, Multnomah County, affected vendors).

2.3 Phase III: Initial Eradication

The Phase III Continued Research and Testing component assumes that the City's Prevention measures are successful. In the event that the City's Prevention measures are unsuccessful, alternative activities are provided.

2.3.1 Continued Research and Testing

- Ensure that updated virus definitions have been distributed. Confirm their effectiveness at the Clean Site.

  Alternative: Obtain inoculation tools and test on server and desktop units.
- Continuously monitor all virus information sources (Web-based, media, IT peers, others).

2.3.2 Eradication

- Based on analysis of pertinent log files and diagnostic procedures, locate and destroy initial and subsequent viral infections to the extent possible.
- Conduct initial meeting of all E-mail administrators: review current status, review common methodology (review citywide coordination protocol, share information, share solutions).
- Obtain and distribute inoculation and eradication tools for remote sites.
- Conduct and support systematic removal from servers.
- Support automatic inoculation and eradication at the workstation level.

2.3.3 Ongoing Testing and Revised Methods

- Test to insure containment and removal using copy of virus.
- Based on field experience and diagnostics, revise eradication methodology rapidly.

2.3.4 Ongoing Bi-directional Notification and Communication

- Routinely update status to BIT Help Desk, City staff, and Commissioners Offices (broadcast Voice Mail).
- Support ongoing bi-directional, routine, planned communication between field staff to insure that coincidental impact and issues are shared.

2.4 Phase IV: Systematic Restoration of Service and Stand-down

- Connect clean[2] workstations to subsystem servers.
- Connect clean subsystem servers to City server.
- Connect City system to Internet.
- De-escalate as appropriate, with continued eradication, testing, and bi-directional communication.

2.5 Phase V: Follow-up and Debrief

- Deliver final 'all clear' notification and acknowledgements.
- Debrief Rapid Response Team, internal bureau support staff and remote site response team members. Modify plan as required.

[2] Clean means that evidence of contamination no longer exists as certified by the appropriate System Administrator.

APPENDIX A: CONTACT INFORMATION

Public Information Officers

Name	Office/Bureau	Phone
Elisa Dozono	Mayor's Office	823-3442
Martha Richmond	PDC	823-3296
Joan Saroka	BES	823-5122
Neil Heesacker	Fire	823-3803
Sgt. Steve Botener/ Henry Groper	Police	
Matt Emlen	Energy	823-7224
Mary Volm	Transportation	823-7785
Amy Schwartz	Planning	823-6143
Ann Kohler	Buildings	823-7886
Karen Loper	Parks	823-5118
Ross Walker	Water	823-7500

Bureau IT Managers

Bureau	Name	Phone	Pager
BES	Debbie Douglas	7762	
BGS/Comm	Nancy Buchanan	4337	
BOEC	Malcolm Pullen	4670	
Buildings	John Coles	7962	
BIT	Dave Hawkins	6906	
Fire	Thanh Nguyen	4574	
ONI			
Parks	Gary Corbin	5236	
PDC	Steve Arndt	3256	
Police	Bill Wesslund	0301	
Transportation	Eileen Argentina		
Water	Steve Fulmer	6977	
ITSP	Art Alexander	4893	

Awareness of National Security Issues and Response (ANSIR) Contact List

(02/07/00)

Glenn Meyer
Bureau of Information Technology
Director
1120 SW 5th Ave, Rm 450
Portland, OR 97204
(503) 823-6920
gmeyer@ci.portland.or.us

Tyson Peterson
Bureau of Information Technology
Senior IT Analyst/Email Administrator
1120 SW 5th Ave, Rm 450
Portland, OR 97204

(503) 823-5662
tpeterson@ci.portland.or.us

Ali Karout
Bureau of Information Technology
Principal IT Analyst/Network Administrator
1120 SW 5th Ave, Rm 450
Portland, OR 97204
(503) 823-6908
karout@ci.portland.or.us

Al Rouse
Bureau of Information Technology
Desktop and LAN Support IT Manager
1120 SW 5th Ave, Rm 450
Portland, OR 97204
(503) 823-6908
arouse@ci.portland.or.us

David Scott Hawkins
Bureau of Information Technology
Technical Services Manager
1120 SW 5th Ave, Rm 450
Portland, OR 97204
(503) 823-6906
dhawkins@ci.portland.or.us

Benny Hoan Tran
Bureau of Information Technology
IT Analyst/Network Specialist
1120 SW 5th Ave, Rm 450
Portland, OR 97204
(503) 823-6969
btran@ci.portland.or.us

Janet Elaine Hargis
Office of Planning and Development Review
Network Services Administrator
1900 SW 4th Avenue, Suite 5000
Portland, Oregon 97201
(503) 823-7478
hargisj@ci.portland.or.us

Karen Hume
Water Bureau
Network Administrator
1120 SW 5th, Room 600
Portland OR 97220
(503) 823-7469
Khume@water.ci.portland.or.us

Terry Kingrey
Portland Development Commission
Principal IT Analyst
1900 SW 4th, Suite 7000
Portland, OR 97201
(503) 823-3253
tkingrey@portlanddev.org

Rudy Sanchez
Bureau of Emergency Communications
Network Administrator
9911 SE Bush St
Portland, OR 97266
(503) 823-4607
rudy@ci.portland.or.us

Stanton Archer
Office of Transportation
IT Principal Analyst
1120 SW 5th, Rm 830
Portland OR 97204
(503) 823-7174
stana@trans.ci.portland.or.us

Gary Corbin
Portland Parks and Recreation
IT Manager
1120 SW 5th Rm 1302
Portland OR 97204
(503) 823-5236
gcorbin@ci.portland.or.us

Nelson Zenzano
Bureau of Portland Police
IT Supervisor
1111 SW 2nd Rm 1156
Portland OR 97204
(503) 823-0442
nzenzano@police.ci.portland.or.us

Mohammad Abudakar
Bureau of Licenses
IT Manager
1900 SW 4th Rm 3500
Portland OR 97201
(503) 823-6911
dakar@ci.portland.or.us

Christopher Cavanagh
Fire and Rescue
IT Analyst
1135 SW Powell Blvd
Portland OR 97202
(503) 823-0132
ccavanagh@fire.ci.portland.or.us

Michael Nichols
Bureau of Environmental Services
IT Analyst
5001 N Columbia Blvd
Portland OR 97203
(503) 823-2467
miken@bes.ci.portland.or.us

RESOLUTION NO. 35870

Adopt Computer Virus Prevention and Recovery Plan. (Resolution).

WHEREAS, the City of Portland seeks to ensure the provision of efficient delivery of information, services and access to government for Portland-area residents, City staff, other governments, and business partners; and

WHEREAS, the expedient delivery of accurate information and quality services depend on the existence and maintenance of a secure, reliable, high-speed Information Technology infrastructure consisting of computers, software, and various data transmission media; and

WHEREAS, computer viruses are executable programs designed to surreptitiously enter computers and computer networks and disrupt or destroy those computers, computer networks, and stored data; and

WHEREAS, there are over 49,000 known computer viruses, and

WHEREAS, the number and sophistication of computer viruses and infection methodologies increases daily; and

WHEREAS, for business purposes there exists a high level of interconnectivity and interdependence among the computer networks in the City of Portland; and

WHEREAS, the disruption or destruction of the City of Portland's computers, computer networks, or data files represent threats to the safety of citizens and the capacity of the City to deliver services; and

WHEREAS, the requirement for the digital delivery of information and services to citizens is expected to steadily increase; and

WHEREAS, the prevention of computer virus infection represents the best protection for the computers, computer networks, and stored data of the City of Portland; and

WHEREAS, City Information Technology policies state that:

a. Employees must not commit or permit any breach of security or any action intended to circumvent or reduce the security of the City's computer and network resources.

b. Employees are responsible for assuring that City-approved anti-virus protections are installed, maintained, and active on every computer workstation.

35870

c. Employees are expected to take all anti-viral warnings seriously and to conform to bureau procedures for reporting and responding to same.

d. Deliberate transmission of computer virus contaminated data will be considered as a breach of security .

WHEREAS, a rapid, organized response to computer virus contamination is required to limit risk, minimize damage, and restore normal operational status as quickly as possible; and

WHEREAS, the Mayor of the City of Portland has directed the Bureau of Information Technology to establish a formal computer virus emergency response plan; and

WHEREAS, the Director of the Bureau of Information Technology has produced a formal Computer Virus Prevention and Recovery Plan (Plan); and

WHEREAS, the Plan has been reviewed and endorsed by the City's Information Technology Executive Committee; and

WHEREAS, the Plan informs all appropriate employees what to do in the event of a major computer virus emergency, how to communicate, and how to escalate through full recovery; and

WHEREAS, the Plan assigns incident command to the BIT Director or designee; and

WHEREAS, the Plan establishes 'IT Emergency' declaration procedures for the Mayor; and

WHEREAS, the Plan calls for assignment of a budget control number to support post-contamination financial and statistical analysis.

NOW, THEREFORE, BE IT RESOLVED that the City Council formally adopts the Computer Virus Prevention and Recovery Plan, attached hereto as Exhibit A; and

BE IT FURTHER RESOLVED that the Plan will be regularly reviewed and updated as required to maintain the highest level of efficacy.

Adopted by the Council, MAR 15 2000

GARY BLACKMER
Auditor of the City of Portland
By
Deputy

Mayor Vera Katz
Office of Finance and Administration
Bureau of Information Technology
TG:GM
March 9 , 2000

Agenda No.

RESOLUTION NO. **35870**

Title

Adopt the Computer Virus Prevention and Recovery Plan (Resolution)

INTRODUCED BY	Filed: MAR 10 2000
Mayor Vera Katz	Gary Blackmer Auditor of the City of Portland
NOTED BY COMMISSIONER	
Affairs	By: Britta Olsen Deputy
Finance and Administration	
Safety	For Meeting of:
Utilities	
Works	ACTION TAKEN:
BUREAU APPROVAL	
Bureau: Office of Finance and Administration-Bureau of Information Technology	
Prepared by Date G. Meyerl 3/9/00	
Budget Impact Review: X Completed __ Not Required	
Bureau Head: Glenn Meyer Tim Grewe Tim Grewe by	

AGENDA		FOUR-FIFTHS AGENDA	COMMISSIONERS VOTED AS FOLLOWS:		
				YEAS	NAYS
Consent X	Regular	Francesconi	Francesconi	✓	
NOTED BY		Hales	Hales	✓	
City Attorney		Saltzman	Saltzman	✓	
City Auditor		Sten	Sten	✓	
City Engineer		Katz	Katz	✓	
				✓	