

Appendix D:

Pandemic Influenza Emergency Information Technology Plan

As a key part of a social distancing response to an influenza pandemic, some City employees may be directed to work from home or may request approval to do so. While telecommuting is not appropriate for all employees, and no employee is automatically entitled to or guaranteed the opportunity to telecommute, the City can expect the number of telecommuters to increase substantially during a pandemic. Most employees who do telecommute will, in order to perform their daily tasks, require access to at least some of the City's information technology resources, such as e-mail, electronic files, and selected business applications. The City must take steps now to ensure that it can meet the communication and access needs of employees working at home during an influenza pandemic.

During an influenza pandemic the City of Redmond may also face difficulty in supporting its extensive and complex IT infrastructure, including hardware, software, and applications. In order to prepare for this challenge and to ensure that it can sustain those systems that support its essential services, the City must prioritize the systems that it will support, and it must document roles, responsibilities, and processes for allocating resources.

To prepare for an influenza pandemic, the City must:

- Ensure that the technology systems required to maintain the City's critical business functions will operate effectively during a pandemic.
- Ensure that City of Redmond employees who have been approved to telecommute can work productively at home by providing them with access to the City IT resources needed to perform their jobs (e.g., files, databases, e-mail and other applications).

This Information Technology Plan supports the City in meeting these objectives by:

- Identifying and prioritizing essential IT systems.
- Allocating responsibilities for system maintenance and operations in the event of an influenza pandemic.
- Providing managers within departments the information they need to determine whether their staff members are good candidates for working remotely, and if so, the best method of providing network connectivity for each staff member.
- Providing the information employees working at home require to connect to the City network and to access City voicemail.
- Outlining responsibilities regarding IT support during a pandemic.
- Describing City strategies for maintaining IT security during a pandemic while enabling more City employees to telecommute.

Allocation of Responsibilities

To ensure that its employees can remotely support its essential services during a pandemic, each City of Redmond department is responsible for completing the following tasks:

- Identification and prioritization of its essential services.
- Identification of the computer applications and systems that are necessary to support essential services.
- Identification of employees who require access to the applications which support essential services.
- Determination of employee business communication requirements, including selection of those individuals who need remote access and determination of their hardware, application, and voice communication requirements.
- Determination of individual employees' method of access to the City of Redmond's network: Web access to Outlook Web Access (OWA) for email only or standard VPN connection for access to essential applications, files, email, etc.
- Establishment and execution of policies and procedures for its employees who may work at home, consistent with City Telework Policy (<http://redweb/programs/CAO/07Teleworking.asp>), regarding:
 - Acquisition of equipment (PCs, laptops, network interfaces, peripherals, accessories, etc.) for employees working at home.
 - Acquisition of software licenses for employees working at home.
 - Establishment of an Internet connection for employees working at home.
 - Support of desktop or laptop PCs for employees working at home.

The Information Services has the following additional responsibilities to:

- Maintain and support the City's telephone system, including providing instructions on how to forward telephones and how to access City voicemail boxes remotely.
- Maintain and support the City's backbone data network.
- Maintain and support the City's VPN remote access technology and procedures.
- Maintain and support OWA for all departments. (Most staff in RPD do not have access to OWA at PD request).
- Maintain and support the I.S. Help Desk for all departments.

Assumptions and Findings

The procedures and recommendations contained in this Information Technology Support Plan are based on the following assumptions:

- **City of Redmond voice and data systems and network infrastructure will remain fully operational.** Although an influenza pandemic is an emergency situation and represents an alternative working environment, it would not disrupt the infrastructure as a natural disaster or terrorist attack might. Staffing and supply chain issues are the primary challenges to ensuring the infrastructure remains operational.
- **It will be difficult, if not impossible, to obtain new communication services quickly once a pandemic influenza emergency develops.** During a pandemic, the impact on service providers coupled with the sudden increase in demand will make it difficult to acquire new services (e.g. high-speed Internet connection at home). An influenza pandemic will affect everyone in the area—local government, businesses, utilities, and

private citizens. Therefore, employees who require an Internet connection, computing or communications device, or other product or service, must acquire, install, and test them well in advance of a pandemic.

- **Technical support will continue to be provided by the Help Desk.** If Support personnel are required to work remotely, Technicians may be required to check email and voicemail for support requests which may result in slightly longer response times.
- **No increase in network bandwidth is required.** Because internal network traffic is not expected to exceed normal levels, it will not be necessary to increase the bandwidth of the network links internal to the City network.

A review of survey results and discussions with departments yields the following additional findings:

- **Most employees who need remote access require access to applications and shared files. These employees will require use of VPN to access the City's network, applications and file resources.** The City provides Virtual Private Network (VPN) access to the City network (except RPD) via the Web. This access method provides a secure means of connecting remote computers to the City's network.
- **A slightly smaller number of employees will need access to e-mail only.** Employees who only need access to email will be served by OWA because it can be used from any PC with an Internet connection. OWA supports attached documents, so OWA users can exchange text documents, spreadsheets, and most other common file types.
- **The City has adequate VPN capacity to handle an increased number of VPN users.** The City's current VPN infrastructure can accommodate 50 - 100 concurrent users, which should be adequate to handle the number of users anticipated by departments to require VPN access.
- **The City's Internet Service Provider (ISP), King County I-Net does not provide sufficient bandwidth to handle a large increase in the number of concurrent users.** The bandwidth provided by King County will only support 20 – 25 concurrent users reliably. An increase in capacity requires switching to a commercial ISP or adding an additional ISP.
- **Information Services is considering providing access to the City's network through a SSL VPN.** Currently, remote access to the City's network requires the use of a City-owned and managed computer. A SSL VPN would allow secure access to the City's network via the web from any computer without the need for a VPN software client. I.S. is currently testing this tool to allow a greater number of employees to work remotely. However, this may not prove to be a viable option.

Remote Communication

The City has established two primary ways of connecting externally to the services of its data network: Outlook Web Access (OWA) and Virtual Private Network (VPN) access. Both of these methods of access are intended to serve a particular set of user requirements.

Employees needing access to e-mail only are good candidates for OWA as they can access the City's e-mail/calendar system from any computer. However, OWA does not provide access to Personal File folders (PSTs). When working remotely, all City employees with e-

mail accounts can access their e-mail and calendar remotely via a Web browser through OWA at <https://owa.Redmond.gov/>.

Employees needing secure access to City applications, data files or other resources in order to perform their job-related duties are good candidates for VPN access using a City-owned laptop.

Most City employees who currently have a laptop also have the VPN software necessary to connect to the City's network. In the case of an influenza pandemic, it is anticipated that many more employees, at their departments' discretion, will require this mode of access to the network in order to remain productive.

During such an emergency, it would be extremely difficult, if not impossible, to obtain new communications services quickly. Therefore, it is imperative that all preparations for remote network access be made well in advance of an emergency that necessitates the use of these services.

Remote Access Requirements Survey

- To support advanced preparations for an influenza pandemic, each department was asked to complete a questionnaire indicating their expected levels of remote access during a pandemic. The results are being compiled and the plan will be updated by mid-November to reflect that information.

Working Offline

While it is important for many City employees to have the option of remote access, all City employees should consider the benefits of working offline (i.e. running applications such as Word on the remote computer without always being connected to the City network.) Often, City employees spend their time on tasks such as writing reports or preparing spreadsheets that do not require access to the network. Working offline in such cases significantly reduces the amount of time the remote worker needs to be connected to the City Network.

The advantages of working offline are as follows:

- There is no network dependency, so users do not have to worry about network problems potentially disrupting their work.
- The security of both the City network and the remote computer is highest when not connected.
- The remote user should experience better performance of individual applications when they are used locally or offline, as compared to using them over the network.

The disadvantages of working offline are as follows:

- Software used while working offline (e.g., Word or Excel) must be installed on the computer that is being used.
- The remote computer must have sufficient disk space for the programs and files.
- The remote worker will not be alerted to incoming e-mail while not connected.
- The computer being used may become subject to public records disclosure laws.

Remote PC Requirements

At a minimum, employees using OWA must have a working computer with a network interface, a standard operating system (Windows, MacOS, Linux, other Unix, etc.) configured for Internet access, and a Web browser (Internet Explorer, Netscape, Firefox, etc.).

Employees accessing the City network via VPN must have a City-owned laptop with the current version of the VPN software

Internet Connectivity

Employees working remotely must also have Internet connectivity. A high-speed Internet connection (a connection capable of providing download speeds in the vicinity of 1 megabit per second or greater) such as DSL (Digital Subscriber Line) or digital cable is preferred, as it will do the best job of recreating the experience of working in the office in terms of system response time. Depending upon the specific needs of the remote worker, a lower speed connection (low-speed DSL or dial-up) may be sufficient to meet business needs.

Network Security

Limiting remote access to the City data network will reduce the security issues associated with remote computing. Nonetheless, employees must take responsibility for the physical security of their remote access computers (preventing loss or theft of the devices and ensuring that they are not accessible for unauthorized use.) Employees must also take reasonable precautions to protect their individual passwords and other access rights and privileges. In addition, employees must safeguard the information with which they are working and shall not copy any personal data (e.g., customer, personnel, or credit card records) to computers provided by the City or their personal machines. Employees should log off the network or OWA when they finish their work, when they take an appreciable break, or when there is a possibility that someone might use the computer while the employee steps away.

Employees are responsible for purchasing and installing anti-virus software on their personally owned computers and keeping the anti-virus definitions up to date.

All remote access to the City's technology resources, regardless if the computer is City-owned or employee-owned, is subject to the City's Technology use policy which can be found at: <http://redweb/InfoServices/City%20Technology%20Policy%20Revised%2007-09-2008.pdf>

Prioritization and Mandatory Restrictions

While Information Services is doing everything to ensure the City's remote access requirements can be met, a combination of increased usage and reduced support staff may affect access and response times. It is possible, therefore, that restrictions may have to be imposed on access to City network services.

The Information Services Manager shall have the authority and ability to rescind or restrict access to the City's data network. (Restricted access may include, for example, limiting some users such as those uploading financial or payroll records to non-peak hours.)

The Information Services Manager shall prioritize access to the following types of users:

1. Network support staff and other technicians whose access is required to maintain and support the City data network, its components, and its access mechanisms.
2. Staff who are directly involved with emergency management and who use the City network to share or communicate information supporting the City's ability to respond to an influenza pandemic.
3. Staff who require network access to perform work in support of essential services related to the health and safety of Redmond residents or the City's workforce.
4. Staff who require network access to perform work in support of other essential services that directly impact Redmond residents.
5. Staff who require network access to perform work in support of essential services that sustain the City's ability to function over time, including human resources, payroll, procurement, and financial services functions.
6. Staff who require network access to perform non-essential but important work that supports the functions of government and the quality of life in Redmond.

Implementation and Testing

Consistent with the lists of responsibilities identified in this appendix, departments are responsible for all employee setup related to remote access, and for ensuring that any employees who will be working at home have successfully tested their connectivity and access. These tests can be performed in the current network environment but should also be conducted from a remote location to ensure proper functionality.

Voice Communication

Most employees who will be telecommuting already have the voice communication devices they will need to work remotely: a home telephone and, in many cases, a cell phone. With their own telephones, City employees will be able to:

- Access the City voicemail system.
- Receive telephone calls automatically forwarded to them from their City phone number. (This option should be used only in exceptional cases, as it places a double-burden on the City phone system.)

Access to the City of Redmond Voicemail Systems

The City voicemail system is expected to be fully operational during an influenza pandemic. However, the way in which the voicemail systems are used may change because many employees will not be working in the office. For example, employees working offsite are likely to rely heavily on voicemail. They may wish to change their greeting to alert callers of their situation and to provide sufficient information to reduce the need for a conversation. They may also wish to include reference to a cell phone number or the number at which they will be working. Note, however, that forwarding a City phone to another number outside of the City's telephone network will completely bypass the City voicemail system. That is, calls will not go to the City voicemail system if the caller is forwarded to a number which is busy or the call is not answered. Only if the number to which the phone is forwarded is a City network number (4 digits) will the voice mail system handle the call properly.

In lieu of call forwarding, it is recommended that employees retrieve voicemail regularly or increase their use of e-mail. These alternatives should be sufficient for most employees to keep in touch with constituents.

Employees who work offsite can access their City voice mail by dialing (425) 556-2150 and following the instructions they will receive at that number.

The voicemail quick reference guide is available at <http://redweb/InfoServices/infosvcs.asp>

Technical Support

Note that because Information Services staffing may be reduced during a pandemic, hours of service may be reduced and response times may be slower than normal.

The influenza virus affects people, not hardware or software. However, increased absences among Application, Support and Network Services may significantly reduce the City's ability to maintain, update, repair, or run its applications or network infrastructure.

Many of the City's essential services are supported through the use of computer applications and some are wholly dependent on those applications for effective service management and delivery.

Therefore, departments are reviewing and prioritizing their applications based on the relationship of applications to the provision of essential services.