Information Technology and Protection Considerations for E-Work Arrangements

Introduction:

E-Work is a flexible work arrangement whereby an employee fulfils his or her regularly scheduled job responsibilities at a remote location which is not operated by the employer – usually an employee's home.

Government's E-Work Sample Agreement states the following:

- "Equipment provided is to be used solely for the purpose of performing the duties associated with the employee's position. The employee agrees to follow the employer's policy on *Equipment and Resource Usage*."

- "The employee must ensure all security guidelines and standards are followed. Security guidelines and standards include but are not limited to: physical and environmental security; data security; software security; communications security; computer virus protection; and license agreements and copyright protection."

Departments are strongly encouraged to consult with the Office of the Chief Information Officer (OCIO) before any e-work arrangements are implemented to ensure Information Technology and Protection (IT/P) considerations are understood and agreed upon by both employees and Departments.

Departments are advised that there may be logistical issues associated with transferring job responsibilities to remote locations, such as an employee's home, that are not operated by the employer. Remote work locations must have the same physical and technical security features found in Government offices. Privacy, confidentiality, integrity, and availability to others of Government information must not be compromised. Support of IT assets in such locations may also be challenging and could result in downtime for the employee that would otherwise not exist in a Government of Newfoundland and Labrador office location.

While there are many other considerations for an e-work agreement, Departments must consider information protection, security, IT supportability and financial costs before undertaking e-work agreements with employees.

Before entering into an e-work agreement, employees and departments should also consider the following IT/P implications.

Information Management/Information Protection Considerations:

- Employees utilizing e-work arrangements must adhere to all OCIO protocols on Information Protection. For more information on policies, directives and guidelines visit the OCIO website at www.ocio.gov.nl.ca/ocio/policies.
- In accordance with OCIO protocols, any employee requiring access or use of Government information from home must use a Government-approved laptop. When accessing network drives the laptop must be used in combination with a secure VPN connection.
- Employees may be granted an exemption from using a Government-approved laptop if absolutely necessary, but authority to deviate must be approved by the deputy minister or designate.
- Before the use of personal/home computers is approved, the department should consult with OCIO. There are inherent security risks associated with personal computer use for the purpose of conducting government business.
    - Personal computers may not have up-to-date security patches, firewall and anti-virus software for the reasonable protection of government information.
    - Personal computers may be running peer-to-peer file sharing programs (Limewire, etc.) or chat programs (MSN, etc.) in which the potential exists for Government information to be compromised.
    - Government information must never be stored on a person's home computer.
    - Government software cannot be installed on personal computers.
- To ensure availability, integrity and restorability of data, employees are encouraged to save files to the network (home drive or departmental share drive) through secure VPN. Employees are reminded that the transport of government data on portable media is required to be done in such a manner as to protect against unauthorized access (e.g. encrypted flash drives). The OCIO can assist with strategies that conform to secure and centralized data storage from remote locations.
- There are risks associated with unsecured home-based wireless networks that could compromise the protection of government information. The risk is greatly reduced when using a secured wireless network or a wired network and are further reduced when using secured wireless/wired in conjunction with secure VPN. Upon request, the OCIO may be able to provide added information on techniques for better securing a home-based network for the purposes of conducting government business.
- Any in-house wireless routers must be provisioned with security features enabled as noted in Appendix A. It is highly recommended that employees who do not have a strong understanding of wireless routers and their secure setup seek the assistance of their Internet Service Provider or a third party local IT company to assist in the setup. The OCIO has a standing offer agreement in place with a local company for IT maintenance and support services. Depending upon location, a technician with

that vendor can be dispatched to the employee's location. Costs associated with the service call will be the responsibility of the department and/or the employee depending on the e-work arrangement.

- Employers should consider the sensitivity of government information before approving e-work agreements. Positions that handle highly sensitive information have higher security risks.
- The physical security of government information from a remote work location should mirror or exceed the physical controls in government offices. Remote locations with inadequate physical security controls could breach the confidentiality, integrity or availability of government information. Consideration must be given but not limited to: documents in transit, storage of final copies, disposal of documents, locked cabinets and shredding equipment.
- Employers should ensure that employees undertaking e-work agreements understand the importance of protecting Government information during the e-work arrangement.
- Employers should discuss how physical and electronic security safeguards will be monitored and managed in remote locations to ensure all reasonable safeguards are implemented accordingly.

Information Technology Considerations - Equipment and/or Internet Connections:

OCIO is not responsible for the following costs. These costs may be covered by the department and/or the employee depending on the e-work arrangement:

- Internet connectivity must be purchased through an Internet Service Provider. All costs associated with the initial setup and all monthly charges are the responsibility of the department and/or the employee.
- The purchase and installation of modems and/or routers required for Internet connectivity are the responsibility of the department and/or the employee.

The purchase or replacement of any hardware/software necessary for an employee to avail of an e-work agreement may be covered by the OCIO if charged against the department's discretionary IT fund and handled through the department's Planning and Service Delivery Committee. If the department has used all of its discretionary funding, equipment may be purchased using divisional funds with Financial Operations/OCIO approval.

The only connectivity to the Government of Newfoundland and Labrador network will be through secure Virtual Private Network (VPN). The VPN request form can be found on the OCIO website at http://www.ocio.gov.nl.ca/ocio/forms/RemoteAccessRequestForm.doc.

Information Technology Considerations - Hardware/Software/Connectivity Support:

- Should an employee experience problems with their Internet connection, including modems and routers, they must contact their Internet Service Provider for support.
- For Government of Newfoundland and Labrador owned hardware (desktops, notebooks, monitors, printers) and/or software, employees working from home should contact the OCIO Service Desk for support either by phone at 729-4357 or by email at ServiceDesk@gov.nl.ca. The Service Desk operates during normal business hours.
- The OCIO will make every effort to resolve support issues over the phone and through the use of remote technologies where possible with respect to Government of Newfoundland and Labrador desktops and laptops (similar to how support would be provided if the user was located inside a government building). Under no circumstance will OCIO staff visit private residences or non-Government of Newfoundland and Labrador buildings/offices.
- If the issue cannot be resolved over the phone and it is determined that the equipment needs to be serviced by a Computer Support Specialist (CSS) the following options will be discussed with the employee:
    - Equipment can be dropped off or shipped to the nearest OCIO location and left for repair or the employee can schedule a service time with a CSS at the nearest OCIO location. Service will be prioritized against all other outstanding support requests. While every effort will be made to address a support issue during the agreed repair time, it may still be necessary for the employee to leave the equipment with the OCIO. This could occur if the nature of the problem cannot be fixed within a reasonable time frame such as requires vendor assistance, requires parts, or repair may run into unapproved overtime. If practical, in cases where an extended repair time is expected, the OCIO will arrange for loaner equipment from the surplus equipment pool.
    - Depending upon the type of equipment, a replacement unit can be sent to the employee's location. The employee will send the faulty equipment back to OCIO headquarters.
    - Depending upon location, a technician from the vendor on standing offer can be dispatched to the employee's location. Costs associated with the service call will be the responsibility of the department and/or the employee depending on the e-work arrangement.
- In some cases when equipment other than desktops/notebooks, such as scanners and printers, need servicing, it may still be necessary for the employee to return the desktop/laptop as well in order to ensure a proper repair is completed.

For more information or to consult with the OCIO regarding e-work agreements, departments should contact the OCIO Client Service Representative for their department.

Appendix A – Wireless Router Configuration (Credit to Bradley Mitchell, About.com with OCIO additions in brackets)

(It is highly recommended that employees who do not have a strong understanding of wireless routers and their secure setup seek the assistance of their Internet Service Provider or a third party local IT company to assist with this setup).

Wireless home networks are quite risky as numerous security problems can exist. Today's Wi-Fi networking products don't always help the situation as configuring their security features can be time-consuming and non-intuitive. The recommendations below summarize the steps you should take to improve the security of your home wireless network. (*Employees working from remote locations should keep current on the latest security standards for wireless communications. Employees should check back with the OCIO for updates to these recommendations throughout their e-work arrangement).*

1. Change Default Administrator Passwords (and Usernames)

At the core of most Wi-Fi home networks is an access point or router. To set up these pieces of equipment, manufacturers provide Web pages that allow owners to enter their network address and account information. These Web tools are protected with a login screen (username and password) so that only the rightful owner can do this. However, for any given piece of equipment, the logins provided are simple and very well-known to hackers on the Internet. Change these settings immediately.
(Administrator password should be a minimum of 10 characters long and a combination of letters, numbers and special characters. The password should not be a dictionary word.)

2. Turn on (Compatible) WPA / WEP Encryption

All Wi-Fi equipment supports some form of *encryption*. Encryption technology scrambles messages sent over wireless networks so that they cannot be easily read by humans. Several encryption technologies exist for Wi-Fi today. Naturally you will want to pick the strongest form of encryption that works with your wireless network. However, the way these technologies work, all Wi-Fi devices on your network must share the identical encryption settings. Therefore you may need to find a "lowest common denominator" setting.
(The wireless device should be WPA2 certified with Advanced Encryption Standard (AES) encryption.)

3. Change the Default SSID

Access points and routers all use a network name called the SSID. Manufacturers normally ship their products with the same SSID set. For example, the SSID for Linksys devices is normally "linksys." True, knowing the SSID does not by itself allow your neighbours to break into your network, but it is a start. More importantly, when someone finds a default SSID, they see it is a poorly configured network and are much more likely to attack it. Change the default SSID immediately when configuring wireless security on your network.

4. Enable MAC Address Filtering

Each piece of Wi-Fi gear possesses a unique identifier called the *physical address* or *MAC address*. Access points and routers keep track of the MAC addresses of all devices that connect

to them. Many such products offer the owner an option to key in the MAC addresses of their home equipment, that restricts the network to only allow connections from those devices. Do this, but also know that the feature is not so powerful as it may seem. Hackers and their software programs can fake MAC addresses easily.

5. Disable SSID Broadcast

In Wi-Fi networking, the wireless access point or router typically broadcasts the network name (SSID) over the air at regular intervals. This feature was designed for businesses and mobile hotspots where Wi-Fi clients may roam in and out of range. In the home, this roaming feature is unnecessary, and it increases the likelihood someone will try to log in to your home network. Fortunately, most Wi-Fi access points allow the SSID broadcast feature to be disabled by the network administrator. *(Network administrator refers to the person setting up the wireless router. In the case of GNL E-Work arrangements that can be the employee, a third party local IT company or the Internet Service Provider).*

6. Do Not Auto-Connect to Open Wi-Fi Networks

Connecting to an open Wi-Fi network such as a free wireless hotspot or your neighbour's router exposes your computer to security risks. Although not normally enabled, most computers have a setting available allowing these connections to happen automatically without notifying you (the user). This setting should not be enabled except in temporary situations. *(During e-work arrangements this setting must remain disabled).*

7. Assign Static IP Addresses to Devices

Most home networkers gravitate toward using *dynamic IP addresses*. DHCP technology is indeed easy to set up. Unfortunately, this convenience also works to the advantage of network attackers, who can easily obtain valid IP addresses from your network's DHCP pool. Turn off DHCP on the router or access point, set a fixed IP address range instead, then configure each connected device to match. Use a *private IP address range* (like 10.0.0.x) to prevent computers from being directly reached from the Internet.

8. Enable Firewalls On Each Computer and the Router

Modern network routers contain built-in firewall capability, but the option also exists to disable them. Ensure that your router's firewall is turned on. For extra protection, consider installing and running *personal firewall software* on each computer connected to the router.
(In cases where an employee's personal computer is being used for e-work, personal firewall must be installed and running on each computer connected to the router.)

9. Position the Router or Access Point Safely

Wi-Fi signals normally reach to the exterior of a home. A small amount of signal leakage outdoors is not a problem, but the further this signal reaches, the easier it is for others to detect and exploit. Wi-Fi signals often reach through neighbouring homes and into streets, for example. When installing a wireless home network, the position of the access point or router determines its reach. Try to position these devices near the centre of the home rather than near windows to minimize leakage.

10. Turn Off the Network During Extended Periods of Non-Use

The ultimate in wireless security measures, shutting down your network will most certainly prevent outside hackers from breaking in! While impractical to turn off and on the devices frequently, at least consider doing so during travel or extended periods offline. Computer disk drives have been known to suffer from power cycle wear-and-tear, but this is a secondary concern for broadband modems and routers. *(While away from your computer for a period of time it is recommended that you log off the network).*