



Data Security

Dave Delaney

August 19, 2008

Topics

- Computer and Internet Use
- Data Security
 - Department of Revenue Policy
 - Sales and Use Tax Division Policy



Computer/ Internet Usage

- Equipment and electronic tools are intended for business-related purposes
- Policy covers work and non-work time
- Limited and reasonable use is permitted
 - Does not result in additional costs of resources or loss of time



Inappropriate Use

- Illegal activities
- Wagering, betting, selling
- Harassment
- Fund raising (not for agency)
- Promotion of religious or political activities
- Commercial activities
- Downloading or installing software
- Non-State employee use (family, friend)
- Storage of files that may be regarded as violent, obscene, pornographic, or discriminatory

Computer/ Internet Use

- Filing your taxes
 - You are allowed to use your state computer to file your income taxes. However, you are not allowed to keep Turbo Tax or other accounting software on your computer
- Games
 - Games are not allowed from the work hours of 7:00 am to 6:00pm.
 - Games are not allowed to be played on your lunch hour or breaks
 - Interactive games are never allowed



Computer/ Internet Use

- All computer and internet use can be tracked and specific sites blocked.
 - All the web sites you visit are tracked
- All equipment and software is State property
 - Example: the email you sent to your friend via your state email is public information
 - All email is considered public record unless proven otherwise



Computer/Internet Use

- Music files-not allowed on MDOR computer
 - May play CD's that are factory or CD-R (can not be re-written)
- Internet radio
 - Due to bandwidth restrictions and increased risk of malicious code, it is discouraged



Personal Phone

- Do not forward your work phone calls to your personal phone
- Do not give taxpayers your personal phone number
- Do not put audit/taxpayer info in your personal PDA or phone (appointments, phone numbers)



Email

- Use Secure email if possible
- Obtain waiver to send non-public info
- Do not use MN email address for personal internet purchases
- Do not click on pop-up's
- Avoid automatic email subscriptions



Department of Revenue Policies


Data Security

- Internal Wireless Policy
- External Wireless Policy
- Mobile Computer Devices and Data Storage Media Policy
- Encryption Policy



Internal Wireless Policy-MDOR

- MDOR has implemented a WLAN as an extension of the Department's LAN.
 - Wireless Trusted Network (Trout)
 - Wireless Guest Network (Gopher)



Wireless Trusted Network (Trout)

- Users must attend Wireless Awareness Training (WSAT)
- All required MDOR security software must be installed, enabled, up-to-date, and properly configured
 - McAfee (red M icon on system tray next to clock)



Wireless Guest Network (Gopher)

- Enables guests to access the Internet inside the building in St. Paul
 - Guest will get a username and password from the front desk



Internal Wireless Network MDOR Policy

- Users may not extend or modify the network
- All wireless devices not owned or directly managed by MDOR must be evaluated and authorized



Internal Wireless Policy-Division

- For internal access, attach only to DOR provided and supported wireless networks
- Security Software must be updated and enabled



External Wireless Policy-MDOR

- Remote or external wireless connection must be done so through a VPN connection to DOR's secure network
- Policy pertains to all wireless and cellular data communication devices, and includes any device capable of transmitting DOR data
 - Example-computers, laptops, PDA's



External Wireless Policy-MDOR

- All transmission and storage must adhere to current agency, state, and federal encryption policies
- Only department hardware and approved software can be used
- All required security software must be installed and enabled
- Only authorized DOR technical staff will install and configure software and hardware on DOR owned devices.



External Wireless-Division

- RSA Tokens (for VPN access)
- Use when connecting to the Citrix Access Gateway
- One time password (new one every 60 seconds)



External Wireless-Division

- Wireless Networks
 - Ad hoc not allowed (computer to computer)
 - Home wireless is allowed (recommend securing your system)
- Use only MDOR issued computers to perform division duties – not your home PC
- Use only MDOR approved equipment with your laptop
- Back up to DOR servers whenever possible, otherwise, back up data to jump drive when in the field



Mobile Computer Devices and Data Storage Media Policy-MDOR

- All devices must be secured by password entry
- Encrypted Data must be secured by password entry
- Data in mobile devices or storage media must be backed up
- Policy covers all devices and storage media
 - Example: computers, disk drives, flash drives



Mobile Computer Devices and Data Storage Media Policy-Division

- Use only MDOR issued devices (no personal computers, PDA, iPhones, iPods, etc.)
- Use only your assigned jump drive—not your personal one or a taxpayer's
 - If you give your jump drive to your taxpayer, it must be empty
 - Do not mail your jump drive to a taxpayer or let your jump drive leave your sight
- Use your cable lock on your laptop to prevent theft
- Lock your computer when not in use (window key + L)



Taxpayer Data

- Taxpayers can give you data on a CD-R, on your jump drive, or via email
- Do not put data onto a CD to give your taxpayer (audit report, spreadsheets, etc)
- Do not mail taxpayer data CD's
 - Return it to your taxpayer in person



Encryption-MDOR

- All laptop hard drives must be encrypted using Pointsec software.
- Jump Drives must be encrypted with Lockngo software when storing taxpayer information
 - New Jump Drive Software is coming - Pointsec Protector



Instant Messaging

- PROHIBITED
- Use of free or 3rd party service providers create disclosure risks
- Use of free IM programs is **prohibited** (examples: Google Talk, Yahoo IM, AIM, Microsoft Messengers)
- Chat room are also prohibited



Data Storage

Inventory of Current Audits

- Keep a current inventory list of your audits on the template and your jump drive
 - Update and print the list whenever you add or delete cases
 - Delete any audits from the template once case has been backed up to the L:\ drive and turned in
- Back up your work daily to your jump drive
 - Copy your files to the L:\ drive when you return to the office



Data Storage

Inventory of Complete Audits

1. Copy the E-Audit folder for the completed case to your L:\ drive and to your unit's Completed folder
2. Delete E-Audit folder and any files from your C:\ drive and jump drive
3. Delete completed case from the template
4. Delete any files for this audit from C:\ Temp folder
5. Delete the E-Audit folder from the L:\ drive after you have been informed by your supervisor that the audit has gone through unit review and has been stored on the M:\ Drive



Completed audits and paper documents

- Taxpayer data must be returned to taxpayers
- Audit information can be given to Supervisor if not imaged or attached to audit to be kept to see if audit will be appealed (90 days)
- Worksheets or custom templates can be kept **ONLY** if taxpayer data is removed
 - File name is generic (no ID number)
 - Taxpayer name and ID is not on information
 - Taxpayer data has been removed (vendor info, etc)



Completed audits and paper documents

- Do not save completed audits to CD's or other folders. If you need an old audit restored, you can request a copy off the M:\ drive.



Data Breach

- This policy addresses the requirements of Minnesota Statutes, Section 13.055, which requires notifications be given to individuals when there is a reasonable expectation that the confidentiality of their data has been breached.
- Users must report any damage to or loss of data that is not public that was located on their wireless device to their supervisor and ISD immediately .
 - Fill out form MN Revenue form SLD-1 (Stolen or Lost Data Report)
- Employees that have violated the policies may face disciplinary action, termination, and/or criminal or civil proceedings.



Thank you!

