COURTWARE
Government Software Solutions

Data Loss Can be Catastrophic to Your Agency's Ability to Operate & Extremely Costly to Recover From In Addition to Unwanted Attention and Bad Press

Your Team Is Responsible For Backing Up Your Data

DATA BACKUP & RECOVERY

Agency Guide to Data Backups & Recovery

2018

Losing Your Agency's Data Would be Tragic, But You Can Avoid It

Common Mistakes That Can Lead to Data Loss:

No Plan in Place

If you are not backing up your data, you are completely at risk.

Inadequate Plan in Place

Maybe you have a plan in place but it lacks elements like regular frequency of backup, offsite secure storage of data, regular testing of recovery and restoration of data.

Un-Tested Plan in Place

If you have not tested full recovery of data from one of your backups then you don't know for sure if your data is protected

Important:

Courtware does NOT retain copies of your data.

Your IT team is responsible for all agency data backups.

Take these Steps to Protect Your Agency's Data

1) Review the free READY.GOV online resource for IT Disaster Recovery Plans. https://www.ready.gov/business/implementation/IT
2) Meet with your IT team to review your current data backup plan
3) Perform a full test of your data recovery from recent backup
4) Schedule regular future tests of your data recovery process
5) Ensure that you have both onsite and offsite secure backups

CryptoLocker & Ransomware

Ransomware and CryptoLocker are viruses that enter a user's computer and network and encrypts the files so that they can no longer be accessed. Strong encryption AES-256 is used making un-encryption impossible. The viruses infect the local machine where it enters as well as attached additional hard drives and network connections. An infected machine may display a message similar to the following indicating that a ransom must be paid to unlock the machine.

Common User Mistakes That Can Lead to Virus Infection & Data Loss

Opening of email attachments

Tip: Only open attachments expected from KNOWN senders. If in doubt, verify with the sender before opening.

Opening of links in emails

Some links in emails can cause a virus to be installed. Do not click suspicious links if you do not know the original sender.

Clicking inappropriate ads web pages or emails

Often users are baited into clicking an ad that then quickly and quietly installs the virus before it is detected. No unnecessary ad clicking!

Network Domain Privileges

Administrator privileges should be limited to just the few users who actually need that level of security, not everyone.

Program Installation Restrictions

Set network permissions to restrict installation of programs without admin privileges

Firewall Intrusion Prevention

Monitor incoming traffic for suspicious activity. Use multiple layers of firewall and intrusion protection devices

Aggressive Anti-Spam Software

Filter emails aggressively for spam to minimize the risk that offending emails get through.

Internet Content Management

ICM solutions such as AVG Cloud Care can add a layer of security around internet browsing

Educate Users & Team On Safe Technology Practices

Nothing can replace a smart, educated and focused user. Almost all virus attacks occur as a result of user error.