



FOR YOUR INFORMATION

Summer 2008

The ITS Microsoft Premier Support Agreement

By Gary LeBlanc

Did you know that ITS manages a Microsoft Premier Support Agreement for the State of Mississippi that covers all things Microsoft? This means support for Microsoft hardware and software plus multiple vendor environment products and services. Currently, ITS, along with ten other agencies and one municipality, participate in this agreement, but the program is open to all state agencies and local governing authorities. Microsoft's Premier Support is a three-pronged approach providing the following:

- 1) Knowledge Transfer
 - Hands-on training
 - Best practices
 - Local workshops
- 2) Direct Support Relationship
 - Dedicated Technical Account Manager (TAM)
- 3) Proactive Services
 - Prescriptive advice and recommendations
 - Health checks and code reviews
 - Design guidance
 - Microsoft solution development and deployment

ITS contracts with Microsoft on a fiscal year basis for a set number of Premier Support hours and then allocates these hours to the

INSIDE THIS ISSUE

The ITS Microsoft Premier Support Agreement	1
Cyber Security Tips	2
What is a HOT SITE DRILL?	4
ITS Launches the New Website	5
Rural Health Care Pilot Program (RHCPP)	5
Online Planning System Updates	6

program participants. The hourly rate is the same for the user needing 10 hours per year as it is for the user needing 60 hours. By aggregating the total hours needed, ITS can contract for the lowest per hour rate possible and pass the savings along to the program participants. Many small users would not be able to afford this type of high-end service without this program, but by aggregating this support across state and local government, many can take advantage of all that Premier Support has to offer.

That's the good news. If you have Microsoft open system needs and want the most encompassing service program available, this program is worth checking out. Gary LeBlanc is the ITS contract and program manager, and Gary would be happy to give you more details and to help you decide if this is a cost beneficial program for you.

For details contact Gary LeBlanc at gary.leblanc@its.ms.gov

Cyber Security Tips

As more business is conducted online, such as banking, shopping and other activities, our personal information (such as name, credit card account, address, etc.) is increasingly utilized. Personal information has become a frequent target for data thieves, and the volume of breaches involving personal information continues to grow. According to the Privacy Rights Clearinghouse, there have been more than 240 million records containing sensitive personal information involved in security breaches to-date nationally.

Many types of organizations are interested in obtaining and using your personal information, and it's important to know what information is being collected, by whom, and how it will be used.

Websites track web users as they navigate cyberspace. Data may be collected about you as a result of many of your routine activities including:

- When you make purchases and pay bills with credit cards, you leave a data trail consisting of purchase amount, purchase type, date, and time.
- When you pay by check, data such as phone number, home address, driver's license number, etc. may often be requested to verify your identity.
- When you use supermarket discount cards, the store is able to create a comprehensive database of everything you have purchased.
- When you surf the web, you leave a significant data trail, such as your name, email address, the Internet address of your computer, the name of your computer, the last time you visited that particular site, and the type of browser and operating system you are using.

When you give money to charities, or when you sign up for a subscription or service, such as a magazine, book or music club, a professional association, or a warranty card, your personal information is often collected and stored.

The following tips should be used to help you manage your personal information wisely, to help minimize its misuse, and to lessen the risk of your personal information being compromised:

- Most legitimate websites include a privacy statement. This is usually a link at the bottom of the home page and details the type of personally identifiable information the site collects about its visitors, how the information is used, including with whom it may be shared, and how users can control the information that is gathered. Be sure to read the privacy statement on websites you are visiting prior to providing any personal information, to understand that entity's policy regarding the protection of data.
- When shopping online, guard the security of your transactions by ensuring the transaction is submitted securely. When submitting your purchase information, look for the lock icon on the browser's status bar to be sure your information is secure during transmission.

According to the Privacy Rights Clearinghouse, there have been more than 240 million records containing sensitive personal information involved in security breaches to-date nationally.

Cyber Security Tips

Continued from page 2

- Periodically check your Internet browser settings (e.g. Security and Privacy) to ensure that the settings are adequate for your level and type of Internet activity.
- If you are not already using anti-spyware or adware protection software, start now. This software is designed to protect against spyware or malware designed to extract private information from your computer without your knowledge. Make sure you keep the anti-spyware or adware protection programs updated.
- Be sure to have a firewall installed and enabled on your computer.
- If you store private data on your laptop or other portable electronic devices (e.g. USB), use encryption software to protect your private data in the event the device is lost or stolen.
- Use strong passwords on all your accounts, such as a minimum of eight characters and a mix of special symbols, letters, and numbers.
- To protect against identity theft, always question someone who is asking you to reveal any personally identifiable information. Find out how it will be used and whether it will be shared with others.
- Keep items with personal information in a safe place. When you discard receipts, copies of credit applications, insurance forms, health records, bank statements, or other personal documents, tear or shred them.
- Before replacing a laptop or desktop computer, be sure to remove all sensitive data.
- Order copies of your free annual credit reports from multiple sources. Make sure they are accurate and include only those activities you've authorized.

References

To learn more about protecting your privacy, you may wish to visit the following sites:

Identity Theft:

www.ftc.gov/bcp/menus/consumer/data/idt.shtm

Consumer Action:

www.consumer-action.org

Privacy Information Center:

www.epic.org

Privacy Rights Clearinghouse:

www.privacyrights.org

World Privacy Forum:

www.worldprivacyforum.org

Free Annual Credit Report:

www.annualcreditreport.com

US-CERT Tips for Strong Passwords:

www.uscert.gov/cas/tips/ST04-002.html

Three additional places to check your credit:

www.equifax.com

www.transunion.com

www.experian.com

Resources

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture.



<http://www.msisac.org>

What is a **HOT SITE DRILL**?

By Mike Hatch



ITS Business Continuity Recovery Services

Maintaining backup data files and being able to use those files to return to normal business processing after a disaster, is a challenge for Business Continuity and Recovery Services (BCRS).

Critical business data should be backed up and stored offsite at a minimum distance of fifteen miles from the primary data center.

During a disaster, some staff members may have to attend to personal family problems related to the critical event. When this occurs, alternate staff or consultants may be used to recover and execute business processes for an interim period of time; therefore, detailed plans for executing the recovery processes should be documented, and this documentation should also be stored away from the primary data center.

The ITS Data Center uses two locations to store critical offsite system and data file backup.

ITS also has a **HOT SITE** contract with IBM that provides ITS with access to a fully equipped, operational data center, in the event the State Data Center is inaccessible or inoperable.

Our contract with IBM was awarded via a competitive procurement. This contract supports a specified subset of the normal ITS' production environment that is capable of running critical state government workloads until repairs are made on our primary data center and we can return to our primary location.

As part of our contract with IBM, we have 72 hours each year that we can use during a **HOT SITE DRILL** to test and simulate the recovery of our systems and applications.

During these drills, the ITS network team is able to establish network connections into the recovered data center that allow application testing to be done from desktops in the Jackson area. Some of our user agencies also participate in these tests for their application recovery.

The most recent of these drills was conducted this year during the week of August 18, when an ITS team travelled to one of the IBM **HOT SITES** with our offsite backup files in order to simulate and test a recovery situation.

One of the biggest challenges of the BCRS process is the synchronization of backup files at recovery time.

When business function processes are tested after the files are recovered, there will typically be out-of-sync data due to the backup schedule synchronization that is only seen during a BCRS test.

This can usually be fixed with specially written programs, but is *best* prevented by a **HOT SITE DRILL** and the testing of application business processes to verify that backups can be used for recovery, or the correction of any out-of-sync or missing files.

ITS Launches the New ITS Website

By Caren Brister and Renee' Murray

ITS launched the new ITS website; the new and improved Mississippi Department of Information Technology Services web site @ www.its.ms.gov. It is our hope that users can easily locate the services and support ITS offers, including educational opportunities, in just one click.

With our customers in mind, our goal is to deliver a useful, relevant, and easy-to-use web site. You no longer have to know *where* in the ITS organization a service is offered in order to find it on the website; you only have to know *what* service you're looking for. This means that the new website is based on ITS services rather than the ITS organization.

With ITS' new web site, you don't have to know who to call, because if you can't find what you're looking for, you can access us using the "Contact Us" link.

In addition, the new ITS site provides extensive opportunities via hot links to search for ways to do business with all of state government.

ITS used Interwoven Teamsite software to design the new website. Teamsite provides two major advantages to anyone wishing to maintain an Internet presence with a customized website. First, with Teamsite, changes can be made without the **expense** of hiring a website developer. Second, these changes can be made without the **long wait times** that can occur when using a developer. Time-sensitive content can be added or changed by anyone with an Interwoven Teamsite license and the requisite training.

ITS is taking advantage of this capability with its own website by training content stewards in all functional areas to manage their data, keeping it current and accurate.

Rural Health Care Pilot Program (RHCPP)

By Kevin Gray

To significantly increase access to acute, primary, and preventive health care in rural America, the Federal Communications Commission has dedicated over \$417 million for the construction of 69 statewide and regional broadband telehealth networks in 42 states and three U.S. territories under the Rural Health Care Pilot Program (RHCPP).

The Commission's RHCPP will connect more than 6,000 public and non-profit health care providers nationwide to broadband telehealth networks. These networks provide patients in rural areas telehealth and telemedicine services from critically needed medical specialists (such as cardiologist, pediatricians, and radiologist), around the clock monitoring of critically ill patients by intensive care physicians and nurses, and the ability to video conference specialists and mental health professionals, often hundreds of miles away.

The networks deliver services efficiently, reduce costs and travel time for consumers, decrease medical errors, and enable health care providers to share critical information. The networks also allow quicker response times during public health emergencies, such as bioterrorism attacks, and pandemics or disease-related outbreaks, through expedited coordination with the U.S. Department of Health and Human Services (HHS), the U.S. Centers for

Rural Health Care Pilot Program (RHCPP)

Continued from page 5

Disease Control and Prevention, and other public health officials.

Two Mississippi projects have been selected as pilots by the RHCPP.

- The “As One–Together for Health” project, developed by the Division of Medicaid, seeks to establish a new statewide, non-dedicated, telehealth network connecting tools, running on commodity Internet and Internet2 connections.
- Upgrades to the existing TelEmergency network at the University of Mississippi Medical Center seeks to extend coverage to approximately 90 mostly rural facilities providing telehealth, web-based patient education, and links to the university’s knowledge base.

Online Planning System Updates

By Kevin Gray

ITS’ Online Planning System is used by agency planners statewide to submit annual IT plan data to ITS. The primary or main planning screen received a face lift, bringing it up to date with the new look of the ITS website. However, the enhancements go more than skin deep. Some function keys were relocated to make room for additional project information, such as



the agency’s project ID number, to be visible from the main planning screen. Relocation of other function keys resulted in an aide to workflow, making the Online

Planning System more efficient than last year’s version.

One enhancement gives the agency planners the ability to set the project status to “Draft”, “Active”, or “Completed” using a drop down menu when editing a project. Allowing the agency planners to select “Completed” for projects that have been submitted, approved, and finished or completed, keeps that project’s total budget from being included in the total budget for their overall plan, yet the project remains listed within their plan for ease of viewing. Projects set to “Completed” will not be set back to “Draft” status during the archive process, which allows agency planners to enter “Completed” once, without the need to manually reset the status after each archive.

Previously, the agency planners would set the projects to “Draft” to keep them within the plan listing, making it difficult for them, as well as ITS planners, to distinguish between old “Completed” projects and truly new “Draft” projects.

There were a number of enhancements made to streamline the Online Planning System for the agency planners this year.

[Online Planning System Updates](#)

Continued from page 6

Another enhancement to workflow gives the planners the ability to attach Word, Excel, and Adobe PDF files to a project. This feature provides an easy way for the agency planners to send additional and/or more detailed information with their projects while in turn giving ITS planners easy access to a complete electronic record of the submitted project.

Feedback from the agency planners regarding the changes has been overwhelmingly positive and has stimulated suggestions for future changes to further increase efficiency. We hope to incorporate many of these suggestions before the next planning cycle in a continued effort to improve upon an already efficient and user friendly Online Planning System.

Your IT Policy and Planning Coordinators

Caren Brister

Strategic Services Division

MS Department of

Information Technology Services

301 N Lamar Street, Suite 508

Jackson, MS 39201

phone: 601-359-9598; fax: 601-354-6016

caren.brister@its.ms.gov

www.its.ms.gov

Kevin Gray

Strategic Services Division

MS Department of

Information Technology Services

301 N Lamar Street, Suite 508

Jackson, MS 39201

phone: 601-359-5221; fax: 601-354-6016

kevin.gray@its.ms.gov

www.its.ms.gov

FOR YOUR INFORMATION

Published by:

Mississippi Department of Information
Technology Services

Contact:

Rhonda Allen
601-359-2655

rhonda.allen@its.ms.gov