SECURE SHRED NEWS

May 2014- Vol. 3, Issue 5

Welcome Farrah Rachel

Welcome to the newest member of the All Points Family!
Farrah Rachel Connelly
6 lbs 11oz
18 1/2 inches.

IN THIS ISSUE

Join Our Mailing List!

Our State-of-the-Art On-Site Shredding Trucks

All Points is proud to have state-of-the-art shredding trucks. Our trucks are fully equipped with video cameras so that you can observe the entire process. We offer the smallest shred size and provide you with a Certificate of Destruction to verify you have properly disposed of your confidential documents. 100% of our paper is recycled - helping your business GO GREEN!

DEAR ALL POINTS SHREDDING CUSTOMER:

Did you know?

30% of hard drives are disposed of while still containing private information. Don't get caught! Call All Points to schedule the safe destruction of your hard drives and other media. We can handle x-rays too!

ALL POINTS now offers Medical Waste services through our new company:

ALL POINTS MEDICAL WASTE

Call today to find out how you can have the same great vendor for both services! 772.263.1209.

Who do you know who needs our services? A referral from you is our greatest compliment!

Call today for a free quote or to schedule and appointment
772.283.4152 or 800.696.8483

Sincerely,

Brian M. Connelly
Owner & President

We Love To Share Our Rave Reviews From Our Loyal Customers!

Brian is extremely responsive and I personally enjoy working with him. He makes my job easier because I no longer have to supervise this vendor.

Jim Smith
Facilities Director
Treasure Coast Hospice

Tip of the Month

Make sure your passwords contain numbers and letters and that they are at least 12 characters long. Don't have your password be the same for everything.

All Points Mobile Shredding

Reasons To Use ALL POINTS:

- Local, Family Owned & Operated company
- Serving South Florida Since 1994
- On-Site Document Destruction
- AAA NAID Certified - Highest Designation in Industry
- Reliable, Friendly Service
- Affordable Prices
- Free HIPAA Compliance Training for Your Office & Staff
- Free Assistance Drafting Policies & Procedures For Handling PHI
- No Hidden Fees: No Fuel Charges, Trip Charges or Transportation Fees, etc.
- No Contracts
- All Drivers/Shred Technicians Served in US Military

We Offer Containers in Three Different Sizes At No Cost!

For more information about our products and services, call 800.696.8483 or go click here to go to our website:
www.ShredWithMe.Com

We now have mini containers too!

Furniture-Style Bin
Capacity: 100 lbs.

65-Gallon Bin
Capacity: 200 lbs.

95-Gallon Bin
Capacity: 300 lbs.

A FEW OF OUR VALUED CUSTOMERS:

Thank you to all our of loyal customers!

- Martin Health Systems
- Treasure Coast Hospice
- Harbor Community Bank
- Seacoast National Bank
- Catalfumo Construction
- Proctor, Crook, Crowder
- LaBovick Law Group

- Atlantic Mortgage
- Martin County School Board
- Martin County Sheriff's Department
- Martin County Clerk of Courts
- Martin County Supervisor of Elections
- St. Lucie Sheriff's Department
- St. Lucie County Health Department
- Treasure Coast Ear Nose & Throat
- Allstate Insurance
- Vought Aircraft

Florida Legislature Seeks to Strengthen Security Law

The Florida House of Representatives unanimously passed the Flordia Information Protection Act of 2014. The bill will now be heard by Governor Rick Scott.

Attorney General Pam Bondi issued this statement "Identity theft wreaks havoc on individuals' lives and can have long-lasting effects. This legislation will better protect Floridians' personal information by ensuring that businesses and governmental entities take certain measures to protect personal information and report data breaches to consumers. The legislation will require 30 days notice to my office when a significant data beach has occurred."

The bill includes the following changes to the current law:

- Requires proper notice to be provided to consumers within 30 days unless good cause is shown for a 15 day delay.
- Requires proper notice to be given to Office of Attorney General for a breach affecting 500 or more individuals.
- Expands definition of personal information to include health insurance , medical information, financial information, and online account information such as security questions and answers, e-mail addresses and passwords.
- Expands data breach to include state governmental entities.
- Requires businesses and state governmental entities to take reasonable measures to protect data.
- Requires Office of Attorney General to provide an annual report to the Legislature regarding data beaches by governmental entities.
- Authorized enforcement actions under Florida's Unfair and Deceptive Trade Practices Act for any statutory Actions.

Full Article Here

Security Tips To Keep You Protected:

These Top Tips Will Go A Long Way To Keeping You Safe!

- Have a strong password of at least 12 characters. No matter how strong an eight-character password is, it can now be cracked in about two hours. A strong 12-character password takes roughly 17 years to crack. Use a pass phrase so you can remember the password: "EyEluv@B@TeCH- SHOW2012!" would be a perfect example.
- Don't use the same password everywhere. If they crack you once, they've got you in other places too.
- Change your passwords regularly. This will foil anyone who has gotten your password.
- Do not have a file named "passwords" on your computer. And do not have your password on a sticky note under your keyboard or in your top right drawer (the two places we find them most

often)!

- Change the defaults. It doesn't matter if you are configuring a wireless router or installing a server operating system. In all cases, make sure you change any default values. The default user ID and passwords are well known for any software or hardware installation. Apple isn't immune either, since there are default values for their products as well.
- Your laptop should be protected with whole disk encryption-no exceptions. Stolen and lost laptops are one of the leading causes of data breaches. Many of the newer laptops have built-in whole disk encryption. To state the obvious, make sure you enable the encryption or your data won't be protected. Also, encryption may be used in conjunction with biometric access. As an example, our laptops require a fingerprint swipe to power on. Failure at that point leaves the computer hard drive fully encrypted.
- Backup media, a huge source of data leaks, should be encrypted. If you use an online backup service, which means you're storing your data in the cloud, make sure the data is encrypted in transit and while being stored. Also, be sure that employees of the backup vendor do not have access to decrypt keys.
- Thumb drives, which are easy to lose, should be encrypted. You may want to log activity on USB ports, because it is common for employees to lift data via a thumb drive. Without logging, you cannot prove exactly what was copied.
- Keep your server in a locked rack in a locked closet or room. Physical security is essential.
- Most smartphones write some amount of data to the phone. Opening a client document may write it to the smart- phone whether or not you save it. The iPhone is particularly data rich. Make sure you have a PIN for your phone. This is a fundamental protection. Don't use "swiping" to protect your phone as thieves can discern the swipe the vast majority of the time due to the oils from your fingers. Also make sure that you can wipe the data remotely if you lose your phone.
- Solos and small firms should use a single integrated product to deal with spam, viruses and malware. For solos and small firms, we recommend using Kaspersky Internet Security 2012, which contains firewall, anti-virus, anti-spyware, rootkit detection, anti-spam and much more. For larger firms, we are fans of Trend Micro.
- Wireless networks should be set up with the proper security. First and foremost, encryption should be enabled on the wireless device. Whether using Wired Equivalent Privacy (WEP) 128-bit or WPA encryption, make sure that all communications are secure. WEP is weaker and can be cracked. The only wireless encryption standards that have not been cracked (yet) are WPA with the AES (Advanced Encryption Standard) or WPA2.
- Make sure all critical patches are applied. This may be the job of your IT provider, but too often this is not done.
- If software is no longer being supported, its security may be in jeopardy. Upgrade to a supported version to ensure that it is secure.
- Control access. Does your secretary really need access to Quickbooks? Probably not. This is just another invitation to a breach.
- If you terminate an employee, make sure you kill the id, and immediately cut all possible access (including remote) to your network. Do not let the former employee have access to a computer to download personal files with- out a trusted escort.
- Using cloud providers for software applications is fine, provided that you made reasonable inquiry into their security. Read the terms of service carefully and check your state for current ethics opinions on this subject.
- Be wary of social media applications, as they are now frequently invaded by cybercriminals. Giving another application access to your credentials for Facebook, as an example, could result in your account being hijacked. And even though Facebook now sends all hyperlinks through Websense first (a vast improvement), be wary of clicking on them.
- Consider whether you need cyber insurance to protect against the possible consequences of a breach. Most insurance policies do not cover the cost of investigating a breach, taking remedial steps or notifying those who are affected.
- Have a social media and an incident response policy.
- Let your employees know how to use social media as safely as possible, and if an incident happens, it is helpful to have a plan of action in place.
- Dispose of anything that holds data, including a digital copier, securely. For computers, you

can use a free product like DBAN to securely wipe the data.

- Make sure all computers require screen saver passwords, and that the screen saver gets invoked within a reasonable period of inactivity.
- Use wireless hot spots with great care. Do not enter any credit card information or login credentials prior to seeing the https: in the URL.
- For remote access, use a VPN or other encrypted connection.
- Do not give your user id and password to anybody. This includes your secretary and even the IT support personnel. None of these safeguards are hard to implement. Unfortunately, even if you implement them all, new dangers will arise tomorrow. The name of the game in information security is "constant vigilance."

ALL POINTS
mobile shredding

100 SW Albany Avenue, Stuart, FL 34994
772-283-4152 / SHREDWITHME.COM

Forward email