PROTECTING LASERS INFORMATION

March 2018

LASERS VPN ACCESS:

Do you have VPN access? If so, congratulations! You have been granted the ability to connect into the LASERS network from outside the office, but there is some responsibility that comes along with this trust. LASERS expects you to keep your computer safe with updated antivirus software, a firewall, and patches in a timely manner.

LASERS POLICIES HELP PROTECT LASERS

When is the last time you checked out the LASERS IT Policy? I know it is not your favorite activity. However, it does provide some valuable information on best practices for protecting critical LASERS assets (i.e. DATA). There is one asset that all organizations (public and private) have in common, and that is their proprietary data. For LASERS, much of this is in the form of PII: member Personal Identifiable Information.

LASERS is making investments to protect sensitive information. Everything from shredding confidential reports, to implementing specialized security software, to watching for possible trouble. Everyone at LASERS must be a part of the team to ensure the safety of our member's PII. If you have not done so recently, take a look at the LASERS IT Policy. Have questions? Stop by IT and anyone would be happy to discuss how the policy protects LASERS.

Remember: You are a member of LASERS too!
Protecting member data is protecting your own as well.

What is PII?

- Personally Identifiable Information (PII) is any information maintained by a company which:
  - can be used to distinguish or trace an individual's identity;
  - is linked or linkable to an individual.

- Examples of PII:
  - Name, Address, SSN, Date of Birth, Phone Number
  - Device specific static identifier (e.g., IP Address, UDID, etc.)
  - Logs of user actions
  - Financial, employment, or location data.

LASERS IT
Making Digital Retirement a Reality