INDEPENDENT INNOVATIVE
SERVICE FLEXIBILITY TECHNOLOGY

AT IMPERIAL PFS®, ONE OF OUR TOP PRIORITIES IS DATA SECURITY AND PROTECTING CUSTOMER INFORMATION

In this complex age of technology, we strive to maintain an industry-standard level of security.

Our IT Department takes the following precautions to protect your information:

- Encrypt all sensitive Customer data in our database.
- Highly restrict access to our database, with Security Committee reviewing access annually.
- Scrutinize IT projects to ensure adherence to best practices.
- Encrypt all Customer communication with IPFS®, and any network interchange external to the IPFS network, over industry-standard secure connections.
- Continually evaluate network and server systems for security vulnerabilities and execute remediation immediately.
- Conduct external, third-party penetration tests to ensure our systems remain protected from emerging technologies that attempt to breach systems.
- Continuously review security news bulletins on emerging security threats and evaluate for vulnerability at IPFS.

While our IT Department works tirelessly to protect your personal information, there are many measures you can take to secure your own data. →

In addition to IPFS security measures, you can take the following steps to protect your own valuable data:

- Do not share your ipfs.com username and password with others.
  - Each member in your agency needs his or her own login credentials to access ipfs.com.
  - Limit account Administrators to one or two people.
- Do not leave your laptop, tablet, or phone on your desk. Lock and secure items when not in use.
- Do not leave sensitive information on a white board, bulletin board, or similarly public space in your office.
- Make sure your computer is running the latest approved security patches, antivirus software, and firewall.
- Consistently upgrade to the latest web browser version available.
- Do not leave information lying on the printer or fax machine.
- Shred all documents containing confidential information.
- Do not create passwords using names of family members, birthdays, or other easily guessable information.
- Avoid storing your password locally (i.e. taped to your monitor or keyboard).
- When accessing websites, ensure the address of the site begins with “HTTPS”. The “S” stands for secure, meaning the website is employing SSL encryption.
- If you receive an error message stating that the “SSL certificate was not issued by a trusted certificate authority” or similar warning, do not continue to the website.
- Do not respond to emails or phone calls requesting confidential company information, including employee information, financial results, or company secrets.

Other resources on cyber security include:

- 10 Basic Cyber Security Measures: https://ics-cert.us-cert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_S508C.pdf
- 10 Steps To Cyber Security: https://www.cyberessentials.org/system/resources/W1siZiIsIjIwMTQvMDYvMDQvMTdfNDdfMTdfNjMwXzEwX3N0ZXBzX3RvX2N5YmVyX3NlY3VyaXR5LnBkZiJdXQ/10-steps-to-cyber-security.pdf