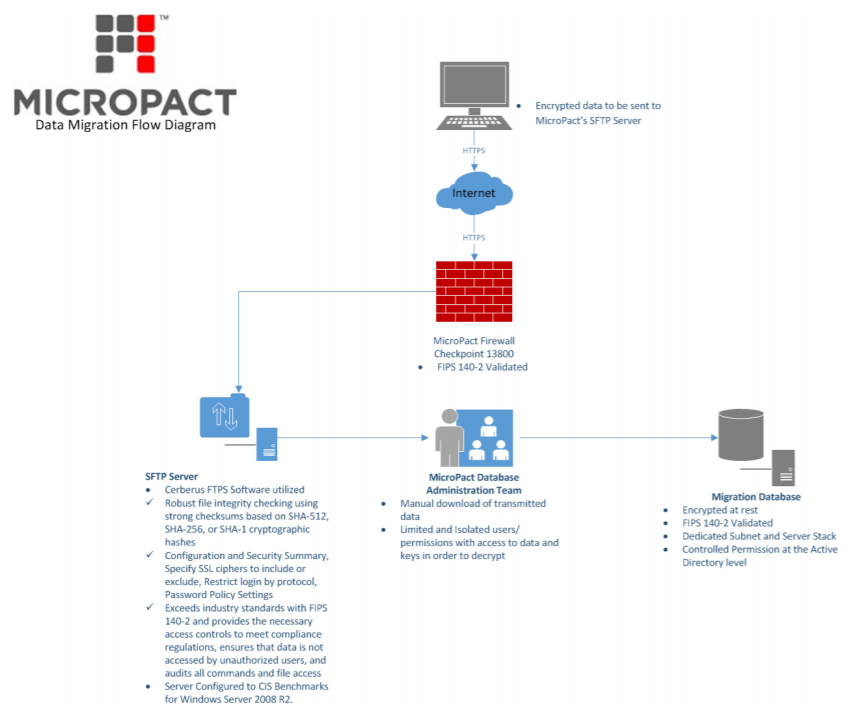
# Platform Security

The SHIP Tracking and Reporting System (STARS) is built using entellitrak, a commercial off the shelf (COTS) tool developed by MicroPact. It has been carefully vetted through security standards as it is a Federal Information Security Management Act (FISMA) moderate system and has been granted Federal Risk and Authorization Management Program (FedRAMP) compliance.

* **MicroPact Data Encryption**
  + Data is encrypted in transit and in while at rest in the database.
  + The MicroPact encryption solution uses Federal Insurance and Mitigation Administration (FIPS) 140-2 validated AES 256-bit encryption on Intel multi-core processors. Intel provides a set of onboard instructions, Advanced Encryption Standard New Instructions (AES-NI), that offload many of the performance-intensive steps to the hardware, so throughput impact is negligible (1–2 milliseconds).





* **FedRAMP Compliance**
  + The Federal Risk and Authorization Management Program (FedRAMP) is an assessment and authorization process which U.S. federal agencies have been directed by the Office of Management and Budget to use to ensure security is in place when accessing cloud computing products and services
  + FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud-based services and products
  + FedRAMP was developed in collaboration with:
    - The National Institute of Standards and Technology (NIST)
    - The General Services Administration (GSA)
    - The Department of Defense (DOD)
    - The Department of Homeland Security (DHS)
  + FedRAMP authorizes cloud systems in a three step process:
    - Security Assessment: The security assessment process uses a standardized set of requirements in accordance with FISMA using a baseline set of NIST 800-53 controls to grant security authorizations.
    - Leveraging and Authorization: Federal agencies view security authorization packages in the FedRAMP repository and leverage the security authorization packages to grant a security authorization at their own agency.
    - Ongoing Assessment & Authorization: Once an authorization is granted, ongoing assessment and authorization activities must be completed to maintain the security authorization.
  + FedRAMP consists of a subset of NIST Special Publication 800-53 security controls specifically selected to provide protection in cloud environments. A subset has been defined for the FIPS 199 low categorization and the FIPS 199 moderate categorization.
  + entellitrak is FedRAMP compliant tool. MicroPact is committed to the FedRAMP program and to keeping the Authority to Operate (ATO) up to date by allowing a neutral third-party assessor to come in and perform critical examinations of their systems.
  + entellitrak is also Accredited and Secure with C&A’s based on NIST 800-53, DIACAP and DCID 6/3.

]

* + <https://www.fedramp.gov/>
* **FISMA Moderate System**
  + The Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, et seq.) is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002
  + The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source
  + In accordance with FISMA, National Institute of Standards and Technology (NIST) is responsible for developing standards, guidelines, and associated methods and techniques for providing adequate information security for all agency operations and assets, excluding national security systems.
  + NIST works closely with federal agencies to improve their understanding and implementation of FISMA to protect their information and information systems and publishes standards and guidelines which provide the foundation for strong information security programs at agencies.
  + NIST performs its statutory responsibilities through the Computer Security Division of the Information Technology Laboratory.
  + NIST develops standards, metrics, tests, and validation programs to promote, measure, and validate the security in information systems and services.
* The top FISMA requirements include:
  + Information System Inventory: Every federal agency or contractor working with the government must keep an inventory of all the information systems utilized within the organization. In addition, the organization must identify the integrations between these information systems and other systems within their network.
  + Risk Categorization: Organizations must categorize their information and information systems in order of risk to ensure that sensitive information and the systems that use it are given the highest level of security. FIPS 199 “Standards for Security Categorization of Federal Information and Information Systems” defines a range of risk levels within which organizations can place their various information systems.
  + System Security Plan: FISMA requires agencies to create a security plan which is regularly maintained and kept up to date. The plan should cover things like the security controls implemented within the organization, security policies, and a timetable for the introduction of further controls.
  + Security Controls: NIST SP 800-53 outlines an extensive catalog of suggested security controls for FISMA compliance. FISMA does not require an agency to implement every single control; instead, they are instructed to implement the controls that are relevant to their organization and systems. Once the appropriate controls are selected and the security requirements have been satisfied, the organizations must document the selected controls in their system security plan.
  + Risk Assessments: Risk assessments are a key element of FISMA’s information security requirements. NIST SP 800-30 offers some guidance on how agencies should conduct risk assessments. According to the NIST guidelines, risk assessments should be three-tiered to identify security risks at the organizational level, the business process level, and the information system level.
  + Certification and Accreditation: FISMA requires program officials and agency heads to conduct annual security reviews to ensure risks are kept to a minimum level. Agencies can achieve FISMA Certification and Accreditation (C&A) through a four-phased process which includes initiation and planning, certification, accreditation, and continuous monitoring.
* <https://www.dhs.gov/fisma>

# Best Practices for Handling Potential Sensitive Data

* **Where to Save Files**
  + Directly onto the computer. Take note of the file destination for deletion if necessary
  + Directly onto an encrypted USB drive for an extra level of security
* **How to Delete Files from a Computer**
  + Locate the saved file in the chosen file destination
  + Once work is completed, navigate back to the file
  + Right click on the file and select “Delete”
  + Locate the Recycle Bin
  + Locate the deleted file in the Recycle Bin
  + Right click on the file and select “Delete”
  + Note: When you delete a file, the operating system does fully remove the file from the disk; it only removes the reference of the file from the file system table. The file remains on the disk until another file is created over it, and it might still be possible to recover data by studying the magnetic fields on the disk platter surface. To ensure the file is unrecoverable, use the assistance of software such as [SDelete](https://docs.microsoft.com/en-us/sysinternals/downloads/sdelete) or [Eraser](https://eraser.heidi.ie/).
  + *The best practices outlined in this document were drafted based on internal guidelines, institutional knowledge, and public information. Internal Health and Human Services (HHS) best practices and guidelines should be leveraged to make the slick sheet adhere to federal standards.*
* **Best Practices for Handling PII**
  + During beneficiary appointments, use private spaces to ensure privacy. If assisters are at an event and a private space is not available, create a space that is out of earshot to discuss private information with potential applicants. Also, use computer screen covers that can help protect PII from the view of others.
  + PII collected from the beneficiary, including name, email address, telephone number, addresses, or other notes must be stored securely.
    - If in hard copy, PII should be stored in locked filing cabinets or within locked offices where the paper filing system is maintained.
    - If in electronic format, PII should be stored securely in a password protected file on a password-protected computer to which only authorized individuals have access.
  + Do not leave files or documents containing PII on desks, printers, personal computers, phones or other electronic devices, and fax machines.
  + Do not send or forward e-mails with PII to personal e-mail accounts (e.g., Yahoo, Gmail).
  + Protect e-mails that contain PII (e.g., encryption).
  + Do not upload PII to unauthorized websites (e.g., wikis).
  + Do not use unauthorized mobile devices to access PII.
  + Lock up portable devices (e.g., laptops, cell phones).
  + Clear your web browser history to avoid other users accessing PII.
  + Disable auto-fill settings on your web browser.
  + Keeping notes might be necessary to perform effective application and enrollment assistance for that beneficiary. For example, a beneficiary’s case may require you to research their specific questions and follow up with them at a later appointment. If a beneficiary provides a general consent for you to gain access to that beneficiary’s PII, you are permitted to keep notes linked to his or her individual situation, unless the beneficiary specifically limits his or her consent to prevent you from doing so.
  + If you write down any quick notes for your own reference during the phone call with a beneficiary but do not intend to keep those notes, shred the notes as soon as you complete the call.
  + All computer equipment, including mobile devices, should have a password-protected login screen that will not allow access to files without the proper, secure password.
  + Any time you step away from a computer, you should lock the computer to avoid the chance that an unauthorized individual gains access to the computer.
  + Always return originals or copies of official documents that contain a beneficiary’s PII to beneficiaries and only make copies for yourself or others if necessary to carry out required duties. It can be helpful to have a supply of manila folders to hand to beneficiaries with their documents inside. This helps them keep track of their documents in one place and shields the content of the documents from view.
  + If beneficiaries mistakenly or accidentally leave behind PII at a facility or enrollment event, store the documents in a safe, locked location, and return PII to beneficiaries as soon as possible.
  + Remind beneficiaries that they should keep their PII locked and in a safe place, or if stored electronically, protected by passwords that they will remember.
  + *The best practices outlined in this document were drafted based on internal guidelines, institutional knowledge, and public information. Internal Health and Human Services (HHS) best practices and guidelines should be leveraged to make the slick sheet adhere to federal standards.*