General Data Security Policy & Procedures Reference Sheet

- Work areas should have a lockable drawer, cabinet, or container where sensitive physical documents should be kept when left unattended. No documents should be left in vehicles.
- Workstation computers should be secured with a strong password known only to the operator. The drives of these computers should be fully encrypted with appropriate encryption software, such as BitLocker or File Vault.
- Strong passwords should include a combination of uppercase letters, lowercase letters, numbers, and symbols. Strong passwords should be updated regularly.
- Workstation computers should be locked using < Windows > + < L > or powered off when left unattended.
- Magnetic media, such as computer hard drives, containing Personally Identifiable Information (PII) should be properly erased with software that will overwrite the information three times before being disposed of.
- Workstation computers should have antivirus software installed. Any attachments downloaded from the internet or email should be scanned with this antivirus software for malicious code prior to opening them.
- When sending emails regarding migrant families or individuals, only use a Unique ID number, such as those assigned by MSIX or MIS2000, to refer to them. Do not include any other forms of Personal Identifiable Information (PII), such as their first name, in the body of your email.
- If Personally Identifiable Information (PII) needs to be sent over email, it should be sent as a password-protected attachment using the tools available in the Microsoft Office suite of applications, or by using a zipping tool such as 7-zip. This password should NEVER be included in the email, and should instead be sent to the recipient through alternative means, such as a phone call.
- If it is suspected that a workstation computer has been compromised, or there is a threat that Personally Identifiable Information (PII) may have been stolen from the workstation computer, then the workstation computer should be immediately disconnected from the internet through appropriate means. The supervisor should be immediately notified, and the workstation computer should remain powered on if possible while disconnected from the internet.
- Any suspicious attempts to request Personally Identifiable Information (PII) by unauthorized parties should be reported to the supervisor.