Policy #: IT.006–Data Security

Governed by: IT Administration	
Approval Date: November 1, 2016	**Last Updated:** November 1, 2016
Purpose: CEO Data Security and Protection	

CEO Data Security and Protection – CEO IT Systems

Users must not send, upload, remove on portable media or otherwise transfer to a non-CEO system any information that is designated as confidential, or that they should reasonably regard as being confidential to CEO, except where explicitly authorized to do so in the performance of their regular duties. CEO employees (users) are expected to exercise an awareness, sense of caution and care when handling a person's information which is not relevant to anyone else, for example personal health information (PHI).Users must keep passwords secure and not allow others to access their accounts. Users must ensure all passwords adhere to the CEO password guidance document, found on the agency's intranet.

Users who are supplied with computer equipment by CEO are responsible for the safety and care of that equipment, and the security of software and data stored on it and on other CEO systems that they can access remotely using it.

Because information on portable devices, such as laptops, tablets and smartphones, is especially vulnerable, special care should be exercised with these devices. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it.

All workstations (desktops and laptops) should be secured with a lock-on-idle policy active after at most 10 minutes of inactivity. In addition, the screen and keyboard should be manually locked by the responsible user whenever leaving the machine unattended.

Users who have been charged with the management of those systems are responsible for ensuring that they are at all times properly protected against known threats and vulnerabilities as far as is reasonably practicable and compatible with the designated purpose of those systems.