Information Systems Program

Privileged-level Access Agreement (PAA)

The following rules of conduct and acceptable use policy apply to all users of the Information Systems Program (ISP) Publications website whether NIH employees or contractors. Because written guidance cannot cover every contingency, you are asked to go beyond the stated rules, using your best judgment and highest ethical standards to guide your actions. These rules are based on Federal laws and regulations and NIH policies. As such there are consequences for non-compliance.

User understands that user has requested access permission to provide data to Information Systems Program (ISP). All data provided represents publications submitted and/or to be submitted to the scientific community on behalf of SAIC-Frederick/Frederick National Lab for Cancer Research (FNLCR).

Acknowledgement of Responsibilities

User will protect the account access and authentication to the highest level of data or resource it secures.

User will NOT share authentication data entrusted for users use.

User is responsible for all actions taken under users account and understand that the exploitation of this account would have catastrophic effects to company reputation, networks and applications for which user has access. User will ONLY use the special access or privileges granted to user to perform authorized tasks or mission related functions. User will only use my privileged account for official administrative actions.

User will not attempt to "hack" the network or applications, subvert data protection schemes, gain, access, share, or elevate permissions to

data or PII for which user is not authorized.

User will immediately report any indication of intrusion, unexplained degradation or interruption of system or network services, illegal or improper possession of content or files, or the actual or possible compromise of data, files, access controls, or systems to helpuser@mail.nih.gov

User will not install unauthorized or malicious code, backdoors, software (e.g. games, entertainment software, instant messaging, collaborative applications, etc) or hardware.

User will not create or elevate access rights of others; share permissions to UI for which they are not authorized; nor allow others access to UI or networks under my privileged account.

User is prohibited from accessing, storing, processing, displaying, distributing, transmitting and viewing material that is; pornographic, racist, defamatory, vulgar, hate-crime related, subversive in nature, or involves chain letters, spam, or similarly related criminal offenses such as encouragement of criminal activity, or violation of State, Federal, national, or international law.

User is prohibited from storing, accessing, processing, sharing, removing, or distributing Classified, Proprietary, Sensitive, Privacy Act, and other protected or privileged information that violates established security and information release policies.

User is prohibited from promoting partisan political activity, disseminating religious materials outside an established command religious program, and distributing fund raising information on activities, either for profit or non-profit, unless the activity is specifically approved by the company.

User is prohibited from using, or allowing others to use, granted resources for personal use or gain such as posting, editing, or maintaining personal or unofficial information or pages, web-blogs, or blogging sites, advertising or solicitation of services or sale of personal property (e.g. eBay) or stock trading.

User understands that all information published, drafted or uploaded is subject to monitoring.

User will obtain and maintain required certification(s) in accordance with NIH policy to retain privileged level access.

User understand that failure to comply with the above requirements is a violation of the trust extended to me for the privileged access roles and may result in consequences in accordance to corporate policy.