7-10-2018

Collaborative Research: Proofing A Basic Systems Engineering Model Through Empirically-Based Cognitive Testing

Kurt Becker
Utah State University, kurt.becker@usu.edu

Data Management Plan

Scope

The source data will be collected by the collaborating institution, Utah State University. The only data generated at UNCC will be analysis data from de-identified sources.

Privacy protection

Collection and handling of sensitive information, including personal identifiable and/or location information, will be carried out in a way that is approved by the University's Institutional Review Board (IRB) and in accordance with relevant federal and state privacy laws and regulations. Electronic data with potentially sensitive information will be encrypted. Only de-identified information will be made available for public dissemination.

ISO 27002 was adopted by UNC Charlotte in the Spring of 2012. All standards and guidelines are based on this code of practice for Information Security Management. The UNC Charlotte Information Assurance subcommittee, made up of representatives from distributed units across campus, meets each month to review and discuss data guidelines and security. UNC Charlotte is finalizing its "Policy on Definition and Classification of Sensitive Information" that establishes a four tier data classification system to map all data on campus into a level ranging from 0 (public) to 3 (access regulated by law or contract). Each data set collected and/or analyzed in the project will be evaluated and assigned a classification level so that appropriately restrictive security measures can be assured for data access, storage and management. The UNC Charlotte "Data Use Requirements Guideline" document is used to assign a system risk designation and define appropriate data use.

Mechanism for data sharing

Publications. Books and refereed publications are made available in accordance to relevant copyright agreements with the publishers.

User study protocols and other user study data may be made available by contacting the Co-PI. User study data will be released in accordance to the governing IRB protocol and in compliance with all privacy laws and regulations. Reasonable costs may be charged for data preparation (e.g. redacting personal information).

Time lines sharing

Data may be requested after publications (technical reports, books, papers, theses and dissertations) and / or submission of NSF reports. Data release may be delayed for a reasonable amount of time when (a) it is related to an invention disclosure, or (b) it is being analyzed for pending publications, in this case it should be no more than two years after the completion of the project.

Intellectual property protection

Data may be withheld when it is part of a pending patent filing. Data must be released no more than 60 business days after the patent decision is made.

Data retention

All generated data will be stored on password-protected computers at the UNC Charlotte. Data will be stored on secure servers and backup disks in the College of Computing and Informatics. All data will be backed-up on a regular schedule in consultation with the technology staff of the College of Computing and Informatics. All reasonable efforts will be made to retain data for at least five years after the completion of the project.