Plan Overview

A Data Management Plan created using DMPTool-Stage

Title: NIST Public Safety Innovation Accelerator

Creator: Matthew Hudnall - **ORCID:** 0000-0003-3063-2458

Affiliation: University of Alabama (ua.edu)

Principal Investigator: Matthew Hudnall

Data Manager: Matthew Hudnall

Funder: National Science Foundation (nsf.gov)

Funding opportunity number: 2017-NIST-PSIAP-01

Template: NSF-CISE: Computer and Information Science and Engineering

Last modified: 02-23-2017

The project PIs, Matthew Hudnall and Jacob Chakareski, will oversee this project and they will assign a qualified data manager who is trained in disclosure risk management to act as steward for the data while they are being collected, processed, and analyzed. All research data collected as part of this project is owned by the University of Alabama. The Principal Investigators of this project will take responsibility for the collection, management, and sharing of the research data Day-to-day quality assessment will be the responsibility of the Lab Director who in turn is overseen by the Project Director.

This project will involve many sensitive data sources from a number of public safety organizations. Every Staff, Faculty, and Student affiliated with CAPS has been FBI fingerprinted and background checked, in addition to undergoing FBI CJIS training, to ensure that they are trained and checked to appropriately handle sensitive data. Data from officer body worn cameras, citations, crash reports, and officer locations/movement will be aggregated into this data repository. CAPS already has the appropriate MOUs and security measures in place to handle these data sources on behalf of law enforcement.

There are many data sources that will be consumed during the course of this project that will not be made available to other researchers due to the sensitive nature of the data involved. There are public datasets, however, like the Alabama vehicle crash data, that CAPS will make public in a de-identified form. The datasets that will be made available though and the time periods, elements, and distribution criteria are at the sole discretion of the agency that has statutory authority over the officer work product.

All data will be stored and maintained on CAPS servers that meet the FBI CJIS security requirements. For raw data with personally identifiable information, the data will be encrypted in transit and while at rest. For aggregate data statistics, the data will be encrypted in transit to preserve data integrity. The data for this project will be rolled into the data enterprise plan of CAPS, which ensures the continued hosting of any project data source for at least 5 years after the end of a project. CAPS has 4 levels of IT managers in its 80 staff that are tasked with ensuring the safe and secure hosting of all data. We also utilizes a quasi-independent data security officer to oversee all adherence to project data plan specifications.

CAPS employs a master security policy that contains 16 subsections that address every aspect of data security in conformance with FBI CJIS and HIPAA policies due to the wide breadth of data we maintain. A brief summary of these policies are outlined below:

The purpose of the *CAPS Information Systems Master Security Policy* is to define the authoritative security stance of the CAPS organization as well as to define organizational expectations with regards to CAPS information systems. The scope of the *CAPS Information Systems Master Security Policy* covers the information systems under the direct management authority of the CAPS organization. This includes hardware, software, networking, security, data, and all other technologies that are specifically managed by the CAPS organization and are either directly connected or remotely accessible that make up the CAPS information system.

In most cases CAPS does not maintain intellectual or physical ownership over the equipment, data, and technologies that comprise CAPS information systems. CAPS only has authority to manage the information systems. Management authority over these technologies comes from either direct purchase by the University of Alabama for CAPS utilization or through authorization given through grants, business associate contracts, or other organizational agreements.

Finally, as a research center on campus at The University of Alabama the Center for Advanced Public Safety falls

under the administrative umbrella of several levels administrative scopes of authority. CAPS is part of the Computer Science department, which is part of the College of Engineering. As a research institute CAPS also falls under the Office of Special Programs for research and grant related activities. And as an entity on campus with computer resources CAPS is associated with the Office of Information Technology as well as Information Security. These associations, among others, must be taken into account with regards to any policies and procedures implemented within CAPS.

The Center for Advanced Public Safety (CAPS) is committed to maintaining confidentiality, integrity, and availability of protected information in CAPS information systems in support of development, production, administration, and support of the organizational mission. CAPS is also committed to minimizing unauthorized access to proprietary information and technology.

CAPS is committed to utilizing a combination of local, state, and federal regulations, security policies, and industry standard best practices in order to help the organization in its commitment to information security. CAPS is also committed to periodic reviews, both internally and externally, of existing systems in order to identify and address areas of improvement as well as researching newer technologies for implementation in the CAPS information systems environment as part of a process of continual improvement and vigilance.

In order to establish a comprehensive security policy the following security framework has been created to provide an outline of the overall security policy as well as pointers to underlying security policies providing more in-depth coverage of specified areas of the CAPS information system.

As a research center on campus under The University of Alabama any policies and procedures implemented for the purpose of managing CAPS Information Systems may not super cede any policies and procedures established by The University of Alabama or parent organization on campus except where required to comply with local, state, and federal regulations related to any protected information under the stewardship of CAPS as part of a research grant, organizational agreement, or related contract with external, non-UA entities.

Below is the comprehensive security policy framework for securing CAPS information system:

- CAPS Information Systems – All policies defined or referenced below are targeted at CAPS information systems which are under the direct management authority of CAPS.
  - Boundaries – the demarcation point between CAPS information systems and non-CAPS information systems, this represents the first line of defense against external threats attempting to compromise information security and the last line of defense against internal threats transmitting protected information outside of CAPS information systems without authorization.
    - **Virtual Perimeter Policy** – the logical boundary between CAPS information systems and non-CAPS information systems. Policies in this area cover the establishment of outer defenses, DMZs/security tiers, and inner defenses to protect the virtual perimeter of CAPS information systems from unauthorized access.
    - **Internal Segmentation Policy** - the internal boundaries between security and functional areas within CAPS information systems. Policies in this area cover the creation of internal segments within the CAPS information systems to protect against internal user accounts or systems that have been compromised and are attempting malicious activities within the boundaries of CAPS information systems. This includes identifying security and functional areas within CAPS information systems and the utilization of physical and logical segmentation technologies to protect against internal malicious activity.
    - **Data Transmission Policy** – the secure transmission of protected information between CAPS information systems and non-CAPS information systems. Policies in this area cover protected

information as it is being transmitted between CAPS information systems and non-CAPS information systems. Transmission can be either electronic, such as over the internet, or physical, such as via a portable storage device or DVD.

- **Remote Access Policy** – secure access to CAPS information systems by authorized users from non-CAPS information systems. Policies in this area cover authorized users accessing CAPS information systems from non-CAPS information systems and the security characteristics of such connectivity necessary to protect against unauthorized access via authorized remote access channels as well as interception of data while it is in transit between authorized users and CAPS information systems.
- **Physical Boundaries Policy** – the physical boundaries and security measures taken to protect CAPS information systems from direct access or tampering by unauthorized users. Policies in this area define the security characteristics of the operational environment of physical devices which represent the physical boundaries of the CAPS information systems. These policies include datacenter and workstation physical security as well as internal wireless networks that extend direct network access beyond the physical boundaries of the facilities hosting CAPS information systems.

◦ Management – represents CAPS information systems-wide management and security policies. Policies in this area cover the management of CAPS information systems as well as areas that apply to all of CAPS information systems such as risk assessments, compliance reporting, password policies, patch management, and contingency planning.

- **CAPS Information Systems Policies Management Policy** – describes the process for creating, communicating, implementing, monitoring, maintaining, revising, and retiring information systems policies that pertain to CAPS information systems. Policies in this area cover all aspects of managing CAPS information systems policies.
- **Hardware** - represents the physical devices in the CAPS information systems that fall under the direct management authority of CAPS. Policies in this area define the management lifecycle and security characteristics of hardware that CAPS has been authorized to manage through grants or other agreements as part of the organizational mission.
- **Software** – Operating systems, services, and applications that provide electronic services to CAPS information systems. Policies in this area define the management lifecycle and security characteristics of software that is part of CAPS information systems under the direct management authority of CAPS.
- **Data Classification Policy** – describes the classification of data that is input, stored, processed, and/or output into, out of, or within CAPS information systems. Policies in this area define the classifications of data in CAPS information systems and the associated security and operational characteristics of systems that host this data while it is input, processed, transmitted, stored, or accessed into, out of, or within CAPS information systems.
- **Identity and Access Management Policy** – describes policies related to identifying users of CAPS information systems and the resources that they are authorized to access as part of their time with CAPS. Policies in this area define the user management lifecycle from new user request through former user deactivation and deletion as well as the general characteristics for user accounts, identity verification, authentication, and access management.
- **Contingency Planning Master Policy** – describes contingency planning and coordination processes to protect CAPS information systems against various contingencies and disaster recovery. Policies in this area define the creation of a systems wide contingency plan that includes limited outages up to disaster recovery.
- **Password Management Policy** – refers to fundamental password management policies for all

hardware-related firmware, appliances, applications, services, and operating systems authentication. Policies in this area define master password policies that are more specifically defined through individual implementation standards and guidelines.

- **Patch Management Policy** – refers to fundamental patch management policies for all hardware-related firmware, appliances, applications, services, and operating systems. These are the master policies that are more specifically defined through individual implementation standards and guidelines.
- **Security Monitoring Policy** – managing characteristics, integrity, access, duplication, monitoring, and mining of security events contained within the various security logs of systems in CAPS information systems as well as approved responses and required notifications in the event of a breach.
- **Risk Assessment Policy** –independent manual verification of compliance with CAPS information systems policies and/or external regulations with clearly defined assessment protocols that are performed on a periodic basis by both internal and less periodically by external resources.
- **Security Awareness and Training Policy** – refers to bringing awareness to current security considerations and providing training on organizational policies and procedures to ensure awareness and compliance. This policy also covers assessing the security knowledge of IT professionals and providing access to information security training on the latest security threats, best practices, and defense techniques.

◦ **Special Considerations for Projects and Grants** – covers special considerations which may arise from contracts, grants, or agreements between CAPS and other organizations. Policies in this area cover any special considerations that arise from these agreements such as required compliance with specific local, state, or federal regulations that are otherwise not applicable to CAPS as an organization. In many cases these special considerations will be reflected in updated policies and procedures with these changes noted in the respective policies themselves.

- From time to time CAPS will have certain projects or grants that have extra security requirements based on the nature of the information being processed or the requirements defined in the project specification
- The extra security requirements will be addressed with special project-specific policies
- Whenever possible and reasonable these project-specific policies will refer back to existing CAPS security policies to prevent duplication of efforts and also to strengthen existing policies
- CAPS security policies can be adjusted to include specialized wording for such special project needs or the special needs can be provided in project-specific based addendums

---