San Jose State University

DATA MANAGEMENT CHECKLIST

For more detailed information about the data management elements listed – including SJSU, CSU, CA State, and Federal requirements – please refer to the Data Management Handbook provided by the Office of Research, Institutional Review Board.

☐ **Conduct a data inventory and assess level of sensitivity**

- Refer to the SJSU Information Classification and Handling Cheat Sheet.
- Classify data elements as level 1, 2, and 3 based on the Cheat Sheet.
- Use our Excel Data Management Plan Template to help document your data inventory and classification activities.

☐ **Determine where data will be stored**

- On institutional or personal devices? What kind of devices and how are they protected? In the cloud? In an institutional or third party repository? On a shared drive? Are there back-ups?

☐ **Determine who will have access and levels of responsibility**

- Who are the research team members, collaborators, consultants, etc.? How will their access be managed?
- Best practices include: least privilege/need to know access; minimal sharing of passwords, coding keys, and decryption keys; use of confidentiality pledges; revoking access when a team member is no longer involved; not lending devices or equipment.

☐ **Determine level of security and level of de-identification**

- Examples of administrative safeguards: security/privacy training, confidentiality pledges.
- Examples of physical safeguards: entry controls, locked storage spaces, screen filters.
- Examples of technical safeguards: passwords, encryption, multi-factor authentication, de-identification of data - refer to our Table of De-Identification Techniques for pros and cons of the various techniques.

☐ **Determine how data will be shared and disseminated**

- Be aware of factors that affect re-identification: small sample sizes, highly detailed contextual information, people in the public eye, open records access requirements, machine readability.

☐ **Determine how data will be transmitted/transferred**

- Wired, wireless, cellular networks? Courier services? How will data be protected? Do you need to protect metadata also?

☐ **Understand obligations for protecting data when traveling**

- Do U.S. import/export control laws apply? What are U.S. custom's inspection rules about accessing devices? What are the custom's rules for the country to which you will be traveling?

- Refer to the ACLU's Traveler's Bill of Rights.
- Refer to U.S. DHHS International Compilation of Human Research Standards.
- Refer to local resources in the country you will be visiting.

☐ **Develop a retention plan**
- Do not confuse "research data" with "personally identifying information." Retention requirements apply to the latter.
- The CSU retention requirement for research records is a minimum of 3 years, but the IRB has ultimate authority over the retention period of PII; it can be less than 3 years in order to protect research participants.

☐ **Understand proper methods for disposing of PII**
- Cross-cut shredding, pulverizing, or burning for paper, optical media (CDs, DVDs), and USB flash drives or thumb drives; software-based, DOD-approved, disk wiping utility for all other digital files.
- Document your process for data destruction and ensure the same for outsourced work through written agreement with the vendor.

☐ **Understand the types of potential threats to confidentiality and privacy of subjects**
- Tampering, alteration, damage, loss, theft of data or equipment; unauthorized access or use; improper de-identification or disposal of data; excessive sharing of passwords; inferential disclosure from statistical properties of the data; reversal of coding techniques.

☐ **Develop an incident response plan**
- Train research personnel→identify breach→assess impact→follow required reporting structures.
- Use our Incident Report to communicate a data breach, data loss, or unauthorized access and use.

☐ **Be aware of any legal and contractual obligations that apply to the data**
- Most relevant federal laws: FERPA, PPRA, HIPAA, COPPA, Civil Procedure and Discovery Rules.
- Most relevant CA state privacy laws: Information Practices Act, Privacy of pupil records – various statutes in CA education code and business professions code, Consumer Privacy Act.
- Most relevant CA state mandatory reporting and disclosure laws: Civil Discovery Act, Child Abuse and Neglect Reporting Act.
- Most relevant international laws: EU General Data Protection Regulation.

☐ **Don't confuse terms like "anonymous", "de-identified", and "confidential"**
- Refer to the glossary in our Data Management Handbook and make sure you use the terms appropriately in your IRB application.