PROTECTING YOUR RESEARCH DATA -- SUMMARY TABLE

	Research Data			
	Does Not Contain Personal Identifying Information (PII)	Contains Personal Identifying Information (PII)		
Sensitivity Level		**Level 1**	**Level 2**	**Level 3**
Definition	Information that contains neither personal identifiers nor enough specific data to allow inference of subject identities	Benign information about individually identifiable people	Sensitive information about individually identifiable people	Very sensitive information about individually identifiable people
Examples	De-identified data from a survey or experiment	Data from a survey about reading habits; data from an experiment on pattern recognition	Data on employment history, personal relationships; data from an experiment on racial attitudes	Data on sexual behavior, illegal drug use, criminal behavior, crime victimization, or data from medical and mental health records
Desktop and laptop computers	Password protected access	Authentication required for access to data; device hard drive configured in a manner consistent with University security practices	Should not be copied to and/or stored on a personal workstation's hard drive unless the Level 2 data is stored on the workstation's hard drive in an encrypted form using encryption technology approved by the Office of Information Technology (OIT).	Storage on personal workstation hard drive is strongly discouraged
File server	Password protected access	Authentication required for access to data; file server configured in a manner consistent with University security practices	Level 1 standard and data stored must be encrypted	Strongly recommended that access to data allowed only through a server (e.g., terminal server, Linux server accessed via SSH) in the University's data center that requires multifactor authentication utilizing a mechanism approved by OIT; all data files must be encrypted
Removable storage media	Physically stored in a secure manner	Physically stored in a secure manner	Content is encrypted and media are stored in a locked file drawer or safe;	Content is encrypted and media are stored in a locked file drawer or safe; use managed in a check in/check out system

Paper forms	Physically stored in a secure manner	Stored in a locked file cabinet in a secure office or building; documents with names and other identifiers physically separated from research data	Stored in a locked file cabinet in a secure office or building; documents with names and other identifiers physically separated from research data	Stored in a locked file cabinet in a secure office or building; documents with names and other identifiers physically separated from research data
Cloud storage services	Password protected access	Secure cloud storage system approved by the Office of Information Technology (OIT)	Level 1 standard and all stored data must be encrypted	Use of cloud storage systems not recommended
Encryption	Use for file transfer	Use for file transfer	Use for file transfer and all data storage; system used for storing passwords must also be encrypted	Use for file transfer and all data storage; system used for storing passwords must also be encrypted
Data transfer	Should be limited to methods that are password restricted or encrypted	Should be limited to methods that are password restricted; data files must be encrypted	Should be limited to methods that are password restricted; data files must be encrypted	Should be limited to methods that are password restricted; data files must be encrypted