ERC Remote Access Researcher Security Agreement

The University of Texas at Austin
Texas Education Research Center

Researcher Name:		UT EID:	
Project Title:		TACC ID:	
		Cell Phone:	
Institution/Organization:		Office Phone:	
Contact Email:		*For ERC Office Use Only:*	
Google Calendar Email:		Proj #/Abbrev:	
Preferred File Format:	☐ SPSS ☐ STATA ☐ SAS ☐ TEXT	Database Amended Date:	
		Assigned Door Code:	

As an "agent" of the UT Austin Texas ERC, you have access to confidential data.
By your signature below, you acknowledge and agree to all of the following Terms and Conditions:

1. Training, Payment & Requirements to Access Data
a. I have accessed & read online at www.texaserc.utexas.edu both the *ERC Policies & Procedures for Approved Projects* and *Understanding Your Access*, and will abide by the terms of these policies and any subordinate processes and procedures.
b. Prior to data access being authorized, I will complete required FERPA training. I will ensure that all research and all research-generated products using the data (papers, abstracts, publications, etc.) are compliant with FERPA and that no information will be released that could identify individuals.
c. Prior to data access being authorized, I will complete the both the required *Masking Guidelines & Techniques Training Module* and the *New User Online Assessment*. I will ensure that all research output/products using the data are compliant with ERC Masking Guidelines & Techniques.
d. Prior to data access being authorized, I will obtain the necessary human subject internal review board (IRB) approval (if required) from my institution/organization, and will supply documentation of such to the ERC.
e. Prior to data access being authorized, I agree to pay the ERC access fee cost.
2. General Agreement Terms
f. I will not attempt to identify individuals or publicly release confidential data.
g. I agree to access and use the confidential data only for authorized/approved research and for the purpose(s) of the study.
h. I understand that I must only access the data at the ERC through my own credentials. Under no circumstances will I log into the ERC under another researcher's account or allow another researcher to log in using my account.
i. I will not allow any person to view my computer if they do not have the required ERC authorization (projects with more than one researcher can view work related to the project).
j. I have read the requirements for remote desktop ethical behavior (See Ethical Behavior for Remote Desktop Data Access, Pg 3 of this agreement and *Ethical Behavior for Remote Desktop Data Access* section in ERC policy documents). I assure I will work in a solitary work environment as described in the ERC requirements and I will not access ERC data when outside of the United States of America and its territories.
k. I will use appropriate safeguards (including Computer Security Requirements listed on page 3 of this agreement) to prevent the use or disclosure of confidential data of individuals by (but not limited to) using physical and technical safeguards to appropriately protect the privacy and integrity of individual-level data that is viewed, analyzed, and/or created under this Agreement.
l. The ERC reserves the right to audit any researcher and their equipment used to access the ERC server to identify and comply with all legal requirements. Audits will be assumed to be electronic audits in most instances.
m. I agree to request via online questionnaire that the ERC review generated research products that use confidential data, and I agree to never remove or publically release output/results or confidential information that have not been approved for release from the physical or electronic workspace of the ERC.
n. I understand that remote access of the data is only allowed from within the United States or its territories. Remote data access from any geographical location outside of the United States or its territories is not permitted.
3. Project Modifications & Conclusion
o. I will provide the ERC with regular updates regarding progress and personnel changes/additions for my research project(s). I understand that I need to seek approval for personnel changes. I realize that new personnel are required to obtain all the training, required paperwork and comply with the ERC policy and procedures required.
p. I understand that the data files I create for this project will be destroyed following the completion of the project. Project statistical code will be stored in *Code to Archive* folders for a limited amount of time by the ERC.

q. Within 60 days of the project end date, I will supply to the ERC the state-required written Policy Brief (4-6 pages) highlighting the findings of my study to be reviewed by the ERC Advisory Board and Director. I understand that Researchers who do not provide the required Brief will not be allowed to access the ERC data for later projects until a research brief is submitted. I understand other final research products (reports, journal articles, book chapters, etc.) must also be made available to the ERC and cooperating agencies as outlined in the *Policies & Procedures for Approved Projects.*

4. Penalties, Data Breach Procedures & Cancellation Terms

r. I understand I may be prosecuted by State officials if I reveal any individually identifiable information furnished, acquired, retrieved or assembled by me or others, under the provisions of Section 183 of the Education Sciences Reform Act of 2002 (P.L. 107-279) and Title V, subtitle A of the E-Government Act of 2002 (P.L. 107-347). The chief executive officer at my institution or organization will be notified if it is determined I have failed to follow data security requirements provided in this agreement.

s. A data breach violates federal law (FERPA), Texas law, and ERC policy. I will report any known or suspected breach of confidentiality to the Director, ERC Admin, or IT Coordinator of the ERC as soon as possible, but no more than 24 hours from the time I become aware of the breach. A breach includes the removal or inappropriate sharing of data. I will submit a written report of the incident to the Director and IT Coordinator (listed below and in *ERC Policies and Procedures for Approved Projects*).
UT Austin ERC Director: Celeste Alexander, celeste.alexander@austin.utexas.edu, 512-471-4528
UT Austin ERC IT Coordinator: Andres Rodriguez, Andres.rodriguez@austin.utexas.edu, 512-471-4739

t. This Agreement may be cancelled by any participating party at any time, with or without cause, upon thirty (30) days written notice to the other parties. The ERC reserves the right to immediately cancel this Agreement should a party, in its sole discretion, determine that student information has been released in a manner inconsistent with this Agreement.

u. I recognize that access to the ERC can be suspended based on any violation of this Agreement.

I,_____(*name of researcher*), do solemnly affirm that when given access to the Texas Education Research Center (ERC) database or files, I will NOT:
(i) Use or reveal any individually identifiable information furnished, acquired, retrieved or assembled by me or others, under the provisions of Section 183 of the Education Sciences Reform Act of 2002 (P.L. 107-279) and Title V, subtitle A of the E-Government Act of 2002 (P.L. 107-347) for any reason other than statistical purposes specified in my ERC Advisory Board approved project;
(ii) Make any disclosure or publication whereby a sample unit, individual, or student could be identified; or
(iii) Permit anyone other than the individuals authorized by the ERC Advisory Board or Director of the ERC to examine the individual data.

I also solemnly affirm that I will follow the guidelines and requirements outlined in this agreement.

Researcher Signature: _____ **Date**: _____

[**Must either be hand-signed or a digitally-certified signature**. The penalty for unlawful disclosure is a fine of not more than $250,000 (under 18 U.S.C. 3571) or imprisonment for not more than five years (under 18 U.S.C. 3559), or both.]

ERC Director Name: **Celeste Alexander, Ph.D.**

ERC Director Signature: _____ **Date**: _____

Texas ERC Director: Dr. Celeste Alexander celeste.alexander@austin.utexas.edu (512) 471-4528 **Emergency Text: (512) 350-8246**	**ERC IT Coordinator II:** Andres Rodriguez andres.rodriguez@austin.utexas.edu (512) 471-4739 **Emergency Text: (512) 665-6919**
▪ Application usage ▪ Data availability ▪ Formats & context ▪ Special requests ▪ Server issues	▪ Application usage ▪ Data availability ▪ Formats & context ▪ Special requests ▪ Set-up/mgmt. of user account ▪ Server environment
ERC Administrative Associate: Belinda Cantu at 512-471-0727 or belindacantu3@austin.utexas.edu	

Computer Security Requirements

1. Use of prescribed methods to keep the confidential data safe in alignment with requirements listed above and below
2. Strong passwords must be used
3. Anti-virus software must be installed and enabled.
4. Antispyware must be installed: Installing and enabling anti-spyware software is required.
5. Vulnerability scan findings for your systems must be regularly reviewed.
6. Per ERC Program Requirements, a screen lock of your session will be activated after 5 minutes of inactivity.

Ethical Behavior for Remote Desktop Data Access

There are ethical and best practice considerations when using administrative data for research purposes. The unique risks and benefits of integrating and analyzing administrative data need to be recognized in order to ensure the ethical use of these data while protecting the confidentiality of the individuals whose private information is contained in the data. Users must ensure the security of the data and confidentiality of the information contained in the data.

1. Researchers must only access the data at the Texas ERC through their own credentials. Under no circumstances will a researcher log into the Texas ERC under another researcher's account or allow another researcher to log in through their account. In addition, no researcher will allow any unauthorized person to view her/his computer if they do not have the required credentials/paperwork (e.g. projects with more than one researcher can view work related to the project).
2. The researcher will access and use the confidential data housed at the Texas ERC only for authorized/approved research and for the purpose(s) of the study.
3. The researcher will not attempt to identify individuals or publicly release confidential data.
4. The researcher must not take pictures, use print screen, or share screens.
5. The researcher must report any known or suspected breach of confidentiality to the Director, ERC Administrator, IT Coordinator of the Texas ERC as soon as possible (but no later than 24 hours after you become aware), including the inappropriate sharing of data.
6. Limit laptop use to a solitary work environment preferably at home, work, or school environment. This is to prevent theft or the ability for "shoulder surfing."
7. Access must be from a location in the United States or its territories.

Appendix A

Advisory Board Policies on Remote Access to the Education Research Centers (found in *ERC Policies & Procedures for Approved Projects*)
Recommendations adopted in full on June 17, 2020

Background

The recommendation from ERC Advisory Board Subcommittee is to allow remote access based on security and other expectations listed below. Remote access to the ERCs is a privilege. Security and access control considerations must always be a priority. The following are recommendations for requirements that must be met by the ERC and/or researcher if remote access is to be allowed. Also, an ERC must be approved for remote access, based on meeting all the required criteria and guidelines. ERCs may request the remote access option at their own discretion.

Remote access privilege policy recommendations from the ERC Remote Access Subcommittee to the ERC Advisory Board (AB), as updated and adopted on 6-17-2020:

Equipment and equipment security recommendations

- Allow approved researchers access to ERC data remotely provided it is through a VPN connection with multifactor authentication using a laptop or desktop computer that meets requirements for security software (antivirus, etc.)
- Limit laptop use to a solitary work environment, preferably at home, work, or school to prevent computer theft and the ability for "shoulder surfing."
- Implement a screen lock so if a researcher leaves a computer for 10 minutes or less, it will lock the screen.
- Ensure that ERCs participate in a yearly DIR state penetration test as part of security requirements (as is current practice)

Additional security recommendations

- Researchers must follow requirements outlined in the ERC's security/confidentiality agreement which must be signed and executed prior to any allowed access to ERC data.
- All access will be removed, both remote and onsite, if remote access policies are not followed; researchers who do not follow required protocols may be denied ERC access for five years or more depending on policy violation at the discretion of Advisory Board, THECB, or ERCs.
- Audit of remote access set-ups is allowable at the discretion of the Coordinating Board (as directed by the Advisory Board, when applicable).
- Access must be from a location in the United States or its territories

ERC Advisory Board (AB) policy and project approval recommendations

- The AB should consider the following categories when reviewing projects for remote access approval: type of project, researchers' background and affiliations, type of data requested, amount of data requested, and sensitivity of data. A matrix with examples under each category may be used for review and updated as needed by the Advisory Board; these categories are to guide discussion and ensure due diligence on the part of the Board.
- Large-scale projects for commercial purposes are limited to on-site access only (not including institutional, local or regional evaluations.
- An email notification which lists new ERC approved researchers must be sent to of all three participating agency AB representatives any time a new researcher or research assistant is allowed remote access to a previously approved remote access project. No more than 5 researchers at a time may have remote access on any given project without approval of the AB.
- Researchers who have not met requirements to submit research briefs as required in rule will be barred from remote access privileges until such briefs are received. New projects will only be allowed remote access privileges if the affiliated researchers have provided the required briefs for completed projects.
- As per ERC statute, a center must comply with rules adopted by the AB to protect the confidentiality of information used or stored at the center to ensure that confidential information is not duplicated or removed from a center in an unauthorized manner. Commissioner directed projects, which are allowed by law and rule without Advisory Board review, will require AB approval to move from onsite access to remote access. Researchers must meet the conditions of the remote access privilege policy guidelines. The Advisory Board may vote to allow for email approvals in cases where project timelines may be adversely impacted.

Agency Decision-Rights

- The three "data owners" (the TEA, THECB, and TWC advisory board members), if unanimously agreed, may deny a proposed project for remote access even if a majority of the AB approves. Onsite access would still be allowed in such a circumstance.