NIST Attestation Language

PI Attestation:

By checking this box, I, as the PI requesting access to these data, attest that all requested data, as well as individual-level data derived from the original data, will be secured, at a minimum, in accordance with NIST SP 800-171 or the equivalent ISO/IEC 27001/27002 standards as stipulated by the NIH Security Best Practices for Users of Controlled-Access Data. Institutions with Plans of Action and Milestones (POAMs) to mitigate security risks will be considered compliant. I further attest that any cloud service provider and/or third-party IT system used for data analysis and/or storage will secure data, at a minimum, in accordance with NIST SP 800-171 or the equivalent ISO/IEC 27001/27002 standards as stipulated by the NIH Security Best Practices for Users of Controlled-Access Data.

By checking this box, I acknowledge that my institution is NOT in compliance with NIST 800-171 or an equivalent security standard (ISO/IEC 27001/27002) or DOES NOT have a Plan of Action and Milestones (POAM) in place to mitigate security risks. I further acknowledge that I am not permitted to download or locally store any controlled-access data, or individual-level data derived from the the original data, under this agreement. All data processing and analysis must be conducted using the in-situ data analysis tools available within the NBDC Data Hub, which provides a secure computing environment for research use.

Signing Official Attestation:

I attest that the recipient(s) listed, including sub-applicants, are currently affiliated with my institution, and the correct institutional email addresses are listed.

I further attest that the lead recipient is a permanent employee of my institution at a level equivalent to, at a minimum, a tenure-track professor or senior researcher. They are not lab technicians or trainees, e.g., post-doctoral or graduate students.

By checking this box, I attest on behalf of this institution that all institutional IT systems, cloud service providers, and/or third-party IT systems used for data analysis and/or storage will secure the requested data, as well as individual-level data derived from the original data, at a minimum, in accordance with NIST SP 800-171 or the equivalent ISO/IEC 27001/27002 standards as stipulated by the NIH Security Best Practices for Users of Controlled-Access Data. Institutions with Plans of Action and Milestones (POAMs) to mitigate security risks will be considered compliant.

By checking this box, I acknowledge that this institution is NOT in compliance with NIST 800-171 or an equivalent security standard (ISO/IEC 27001/27002) or DOES NOT have a Plan of Action and Milestones (POAM) in place to mitigate security risks. I further acknowledge that recipient(s) listed here are not permitted to download or locally store any controlled-access data, or individual-level data derived from the original data, under this agreement. Recipient(s) may only process and analyze data using the in-situ analysis tools available within the NBDC Data Hub, which provides a secure computing environment for research use.