Entrepreneurship in the Population Survey

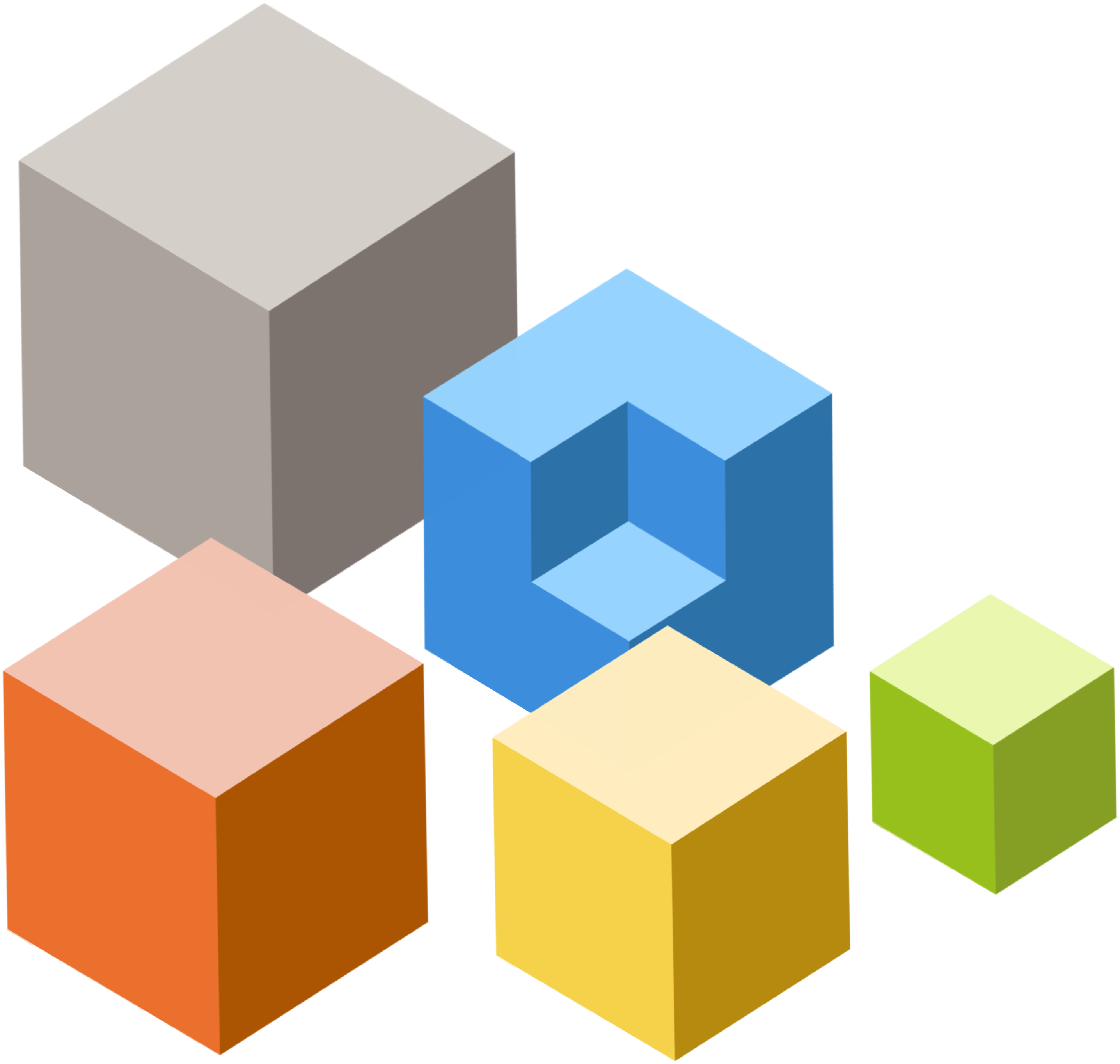
EPOP: Data User Agreement

Attachment B - Data Security Requirements for RUF Access

Issued Date:
October 12, 2022

Created by
NORC at the University of Chicago
55 East Monroe Street, 30th Floor
Chicago, IL 60603
(312) 759-4000 Main
(312) 759-4004 Fax

Point of Contact
The NORC EPOP Research Team
EPOPresearch@norc.org



DATA SECURITY REQUIREMENTS FOR RUF ACCESS

1. **Security of NORC Data:** To prevent loss and unauthorized access or disclosure, DATA RECIPIENT shall use current State or Federal regulation required controls to secure the Data Set.

2. **Security Assessment:** DATA RECIPIENT shall conduct an annual security assessment to identify the security risks to the Data Set. Identified risks shall be addressed through documented remediation plans that shall be made available to NORC upon request.

3. **Security Officer:** DATA RECIPIENT shall appoint a designated Security Officer or specialist who is responsible for compliance with and enforcement of applicable current State or Federal regulations (i.e. NIST, HIPAA).

4. **Policies & Procedures:** Security policies and procedures shall be implemented by DATA RECIPIENT to document the administrative, technical and physical controls in place to protect the Data Set. DATA RECIPIENT shall provide a summary of those policies and procedures to NORC as part of its application for the Data Set. A sanction policy shall be included which outlines appropriate disciplinary actions to address Data set security violations. If DATA RECIPIENT is granted access to the NORC network, compliance with NORC security policies and procedures is mandatory.

5. **Awareness & Training:** An EPOP-specific data security awareness and training program shall be executed by all personnel working with the Data Set prior to contact with the Data Set.

6. **Security Monitoring:** DATA RECIPIENT shall continuously monitor security events and conduct periodic reviews of its information system activities. Any suspicious events shall be investigated.

7. **Incident Response:** DATA RECIPIENT shall implement and maintain a security incident response program that includes:
   a. Notification to NORC at EPOPresearch@norc.org once a Data Set is known to be or suspected to have been compromised. Notice shall be provided to NORC as soon as possible after the DATA RECIPIENT becomes aware of a known or suspected Data Set breach but no later than within 24 hours after DATA RECIPIENT first became aware that a Data Set breach may have occurred;
   b. Identifying containment and mitigation steps to prevent further damage from an incident; and
   c. Corrective action steps to prevent a similar incident from recurring.

8. **Facility & Workstation Security:** For any DATA RECIPIENT facility containing personnel or systems used in the viewing, processing, or storing of Data Sets, the DATA RECIPIENT shall implement the following security requirements:
   a. All exterior doors shall be constructed to prevent unauthorized access and resist

forced entry. Doors shall be alarmed and/or monitored.

b. Access to DATA RECIPIENT facilities shall be restricted in a secure, auditable manner. All personnel should have a unique key, access card, or key code assigned to them. Physical keys are not permitted for data center access.

c. A process for logging and escorting visitors shall be implemented that requires visitors to:
   - Sign in and out
   - Produce photo identification
   - Be escorted at all times
   - Only be granted access for specific, authorized purposes

d. Workstations performing NORC related functions shall be positioned so that the Data Set is not visible to unauthorized personnel.

e. All paper forms or other portable media containing the Data Set must be stored in controlled, secured areas when not in use.

f. DATA RECIPIENT personnel must lock their workstations when they are away from their desks. Workstations shall be configured to automatically lock after no more than 10 minutes of inactivity.

g. The Data Set should not be printed unless in aggregate format.

h. Print capability shall be limited to printers located within DATA RECIPIENT's facilities.

i. Portable storage device drives shall be disabled unless encrypted (i.e. USB, CD/DVD).

j. End-point firewalls shall be installed and configured to prevent unauthorized network access attempts on all DATA RECIPIENT workstations containing the Data Set.

k. Operating systems and application software used must be currently supported by the manufacturer, if applicable.

9. **Encryption:** For Data Sets in transit, DATA RECIPIENT must use encryption technologies that comply with NIST Federal Information Processing 140-2, Security Requirements for Cryptographic Modules. Data Sets at rest must be encrypted in compliance with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices. Additionally, remote access to systems or networks that contain the Data Set must use an encrypted connection.

10. **Anti-Malware:** Servers and workstations involved with accessing, processing, transmitting or storing the Data Set are protected with up to date anti-malware software. DATA RECIPIENT shall have a process in place for issuing regular updates to anti-malware software and conducting regular scans of the environments containing the Data Set.

11. **Access to Data:** DATA RECIPIENT agrees to maintain the following controls:

a. Appropriate authentication controls must be utilized when accessing the Data Set as well as for systems that contain the Data Set.

b. DATA RECIPIENT systems used to access, process, transmit or store the Data Set shall have access terminated as immediately as possible when necessary.

c. DATA RECIPIENT shall notify NORC within 24 hours of any personnel that has access to the NORC network has left the project or is no longer employed by DATA RECIPIENT.

d. Conduct periodic reviews of access to the Data Set, at least annually.

e. Each researcher who shall be using, processing, or storing the Data set shall be issued a unique user identifier and strong password controls are required.

12. **Storage Restrictions:** DATA RECIPIENT shall not transfer, access, or maintain the Data Set or any portion of the Data Set in the cloud based system unless the DATA RECIPIENT is using a FedRAMP-certified cloud service that has been approved for data storage use by NORC. The DATA RECIPIENT shall not transfer, access, or maintain the Data Set or any portion of the Data Set in a location outside the U.S. without prior written consent from NORC.

13. **Patch Management:** A patch management policy and process must be in place which ensures all current patches are applied in a timely manner for all systems and applications related to the Data Set.

14. **Network Security:**

a. DATA RECIPIENT shall implement and maintain strong network security controls to monitor the network and detect any anomalies to be addressed through the formal incident response process.

b. Networks that contain the Data Set must be separated from public networks by a firewall to prevent unauthorized access from the public network. The Data Set must not be stored on Internet accessible networks or network segments.

15. **Disaster Recovery:** Intentionally omitted.

16. **Data Backup/Data Destruction:** The DATA RECIPIENT is permitted to back up the Data Set for purpose of protection against a system failure. The backup copy of the Data Set must be held to the same level of security requirements as the production Data Set. All backup copies of the Data Set must be securely destroyed at the end of the DUA. Upon request, DATA RECIPIENT shall provide confirmation of destruction to NORC.

17. **Data Merging:** The DATA RECIPIENT is prohibited from merging or linking the Data Set with other studies' RUFs. Merging or linking to other public use data files requires prior approval from NORC.