DSS SOUTH CAROLINA
DEPARTMENT of SOCIAL SERVICES

**HENRY McMASTER,** GOVERNOR
**MICHAEL LEACH,** STATE DIRECTOR

Acceptable Use Policy for External Access

Our intentions for publishing this Acceptable Use Policy (AUP) are not to impose restrictions that are contrary to SC Department of Social Services (SCDSS) established culture of openness, trust and integrity, but rather to protect SCDSS employees, partners and the agency from illegal or damaging actions by individuals, either knowingly or unknowingly.

An individual requesting access to the SCDSS network or application must read this AUP and agree to abide by these rules by signing this document and submitting it.

1. You are receiving (SC CACFP) a limited grant of access to resources on the SCDSS network. This account belongs to you and is for your use only. No other individual may access or use this account on your behalf. A violation of this requirement may result in termination of your access.
2. You understand may have access to sensitive information including but not limiting to the following data elements:
    - Personally Identifiable Information (PII)
    - Personal Health Information (PHI)
    - Federal Tax Information (FTI)
    - Criminal Justice Information System (CJIS)
    - Financial
    - Legal
    - Payment Card Industry (PCI) data
    - Agency proprietary information
3. Before you are granted potential access to the above sensitive information, you must ensure and demonstrate through legal and/or technical means that this information is protected in accordance with Federal, State, and Agency standards.
4. You have a responsibility to promptly report the theft, loss or unauthorized disclosure of any sensitive information related to your SCDSS access. In no way should your report to the Agency CISO of such loss exceed 24 hours from your awareness of the loss or disclosure.
5. By signing below, you are acknowledging that SCDSS and the Office of the CISO reserve the right to audit system access and usage on a periodic basis to ensure compliance with this policy.
6. Under no circumstances will you engage in any activity that is illegal under local, state, federal or international law while utilizing SCDSS owned resources.
7. You may not reveal your password to others or allow use of your account by others. This includes family and other household members when work is being performed at home.
8. The data you access may not be given to potential vendors of DSS or other third parties.

The Office of the CISO will certify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner. Any exception to the policy must be approved by the SCDSS Chief Information Security Officer. Any individual found to have violated this policy may be subject to disciplinary action, up to and including termination of resource access.

To report a security incident, please send an email to CISOoffice@dss.sc.gov. Please include your name and a number where you may be reached. Provide as much information as possible regarding the incident, including screenshots.

By signing below, you acknowledge that you have read the above AUP and will abide by the standards listed, and that violating the above AUP could result in loss of access.

The Organization's Authority Employee (Requestor's Supervisor, Manager, Director, etc) acknowledges the request for access to SCDSS network or application and that the employee will abide by this AUP.

Requestor's Printed Name:_____

Requestor's Signature:_____Date:_____

Organization's Authority Employee Printed Name:_____

Organization's Authority Employee Signature:_____Date:_____