EXHIBIT C: Boulder County Data and Cyber Security Requirements

Boulder County (County) requires that its business partners comply with the County's data and cyber security standards while under contract with the County. Contractor shall comply with the following requirements:

Personal Identifying Information and Personal Information Responsibilities

Contractors with access to personal identifying information (PII) or personal information (PI) of Colorado residents, including County employees, or County systems with access to that data shall implement and maintain security, consent, and marketing procedures and practices to protect that data in accordance with Colorado privacy statutes, C.R.S. § 24-73-101 *et seq*. Contractor must be willing to attest that it is complaint with Colorado privacy statutes. Legal requirements may differ based on the agreed-upon work ("Products and Services") to be performed.

Purchasing Card Industry (PCI) Compliance

Contractors that perform work related to purchasing cards shall deliver Products and Services to the County in strict compliance with the Payment Card Industry Data Security Standard (PCI-DSS). The design and standard implementation of the Products and Services must not result in the need for the County to implement compensating controls to maintain the County's compliance with the PCI-DSS. Contractors executing payment processing services on behalf of the County must provide County with access to documentation of its Purchasing Card Industry Data Security Standard Attestation of Compliance (PCI-DSS-AOC).

Criminal Justice Information Systems (CJIS)

Contractors with access to state or federally derived background check data or County systems with such access agree to deliver Products and Services that strictly comply with the FBI's CJIS Security Policy. Without limiting Contractor's obligations hereunder, Contractor agrees to cooperate with County procedures for CJIS compliance that may include, but are not necessarily limited to, background checks and fingerprinting. Contractor is responsible for all CJIS compliance requirements.

Health Insurance Portability and Accountability Act (HIPAA)

Contractors that require access to Protected Health Information (PHI) or County systems that contain PHI shall enter into a HIPAA Business Associate Agreement with Boulder County prior to obtaining the necessary access.

Children's Online Privacy Protection Act (COPPA)

Contractors with access to PI about any child(ren) under the age of thirteen (13) or County systems that contain such data shall implement and maintain security, consent, and marketing procedures and practices in accordance Children's Online Privacy Protection Act (COPPA), 15 U.S.C. § 6501 *et seq*. *See* 15 U.S.C. § 6501(8).

Hosted Information Technology Services (Software, Data, or Infrastructure)

Contractors providing hosted information technology services for the County shall provide documentation attesting to their reasonable security procedures, as well as any non-confidential specific industry attestation (such as a SOC2 Type 1 report) documentation. Contractors providing hosted information technology services agree to maintain an incident response practice to protect hosted County resources.

Data Confidentiality and Integrity

Contractors who host or have access to County data shall control for the integrity and confidentiality of that data by implementing logging, access control, least privilege, encryption in transit, and encryption at rest. Any multi-tenant solution shall enforce the strong separation of County data and systems from those of other customers.

Contractors agree to securely delete all County data within their environment within 90 days after the termination of the parties' agreement or the retention period required by law, whichever is longer. Contractors with access to County access control or authenticity mechanisms (passwords, encryption keys, certificates, or application program interface (API) keys) or who generate them on behalf of the County must implement reasonable security practices to protect the confidentiality of that data. Exposure of a County access control or authenticity mechanism must be reported to the County within three (3) business days.

If Contractor becomes aware that the security of any PII or PI may have been compromised, Contractor will, at its expense: (i) notify County in writing of the occurrence immediately; (ii) address the cause of the occurrence to the extent practicable (iii) cooperate with County's efforts to respond to the occurrence, including sharing with County information relevant to the occurrence; and (iv) reimburse the County for expenses incurred due to the occurrence.

Remote Access to County Resources

Contractors seeking external access to the County's technology resources must enter into a separate Connected Partner Agreement with Boulder County prior to obtaining such access.

Federal Tax Information

Contractors with access to Federal Tax Information (FTI) or County systems that contain FTI data agree to deliver Products and Services that strictly comply with Title 45 Code of Federal Regulations (CFR), Parts 302, 303, 307.