Exhibit 18

AVIATION SECURITY PROCEDURES FOR CONTRACTOR AND SUBCONTRACTOR WORKER BACKGROUND SCREENING

1. CONTRACT WORKER BACKGROUND SCREENING: Contractor agrees that all Contract Workers that Contractor allows to perform work under this Contract shall be subject to background and security checks and screening (Background Screening). Contractor must pay for the cost of all Background Screenings, unless otherwise provided in the Scope of Work. Contractor agrees that Background Screenings required by this Section is necessary to preserve and protect public health, safety, and welfare. The Background Screening requirements set forth in this Section are the minimum requirements for this Contract. The City does not warrant or represent that the minimum requirements are sufficient to protect Contractor from any liability that may arise out of Contractor's work under this Contract or Contractor's failure to comply with this Section. Therefore, in addition to the Background Screening measures set forth below, Contractor and its Contract Workers shall take such other reasonable, prudent, and necessary measures to further preserve and protect public health, safety, and welfare when providing work under this Contract.

As used in this Section, "Contract Worker" means a person performing work for the City, including (1) a person or entity that has a contract with the City, (2) a worker of a person or entity that has a contract with the City, (3) a worker of a subcontractor of a person or entity that has a contract with the City, and (4) a worker of a tenant of the City. (City of Phoenix A.R. 4.45)

1.1. City Rights Regarding Security Inquiries: The City reserves the right to require Contractor to:

1.1.1. Have a Contract Worker provide fingerprints and execute any document that is necessary to obtain criminal justice information pursuant to A.R.S. § 41-1750(G)(4) or Phoenix City Code § 4-22 or both;

1.1.2. Act on newly acquired information, whether or not the information should have been previously discovered;

1.1.3. Unilaterally change its standards and criteria related to the acceptability of Contract Workers; and

1.1.4. Object, at any time and for any reason, to a Contract Worker performing work under this Contract, including supervision and oversight services.

1.2. Contractor Certification: By entering into this Contract, Contractor certifies that Contractor has read the Background Screening requirements and criteria in this Section, understands them, and that all Background Screening information furnished to the City is accurate, complete, and current. A Contract Worker that is rejected for work under this Contract shall not perform any work under any other contract or engagement Contractor has with the City without the City's prior written approval.

1.3. Contractor's Contracts and Subcontracts: Contractor shall include the terms of this Section for Contract Worker Background Screening in all contracts and subcontracts for work performed under this Contract, including supervision and oversight services.

1.4. Materiality of Background Screening Requirements and Indemnity: The Background Screening requirements of this Section are material to the City's decision to enter into this Contract. Any breach of this Section by Contractor shall be deemed a material breach of this Contract. In addition to any other indemnification provision in this Contract, Contractor shall defend, indemnify, and hold harmless the City from and against any and all claims, actions, liabilities, damages, losses, and expenses (Claims) arising out of this Background Screening Section, including the Contractor's disqualification of any Contract Worker or the City's failure to enforce this Section.

1.5. Continuing Duty and Audit: Contractor's obligation to ensure that all Contract Workers pass a Background Screening pursuant to Section shall continue throughout the entire term of this Contract. Contractor shall immediately notify the City of any change to a Contract Worker's Background Screening. Contractor shall maintain all records and documents related to all Background Screenings and the City reserves the right to audit Contractor's compliance with this Section.

2. CONTRACT WORKER ACCESS CONTROLS AND AIRPORT SECURITY BADGE REQUIREMENTS: Contractor shall not allow a Contract Worker to begin work under this Contract until Contractor has completed the Background Screening required by the City and the City has issued the appropriate airport security badge to the Contract Worker. The airport security badge will grant the Contract Worker unescorted access authority only to the area or areas of the Airport that the Contract Worker must enter in order to perform work under this Contract. When a Contract Worker's work in any area ends, the Contract Worker's access authority to that area ends. Any Contract Worker that attempts to enter a restricted area or sterile area, as those terms are defined below, of the Airport without proper authority is an immediate breach of this Contract.

3. **SECURITY IDENTIFICATION DISPLAY AREA (SIDA) BADGE PROCESS:** Each Contract Worker that needs unescorted access authority to a restricted or sterile area of the Airport in order to perform work under this Contract must receive a security identification display area (SIDA) badge from the Aviation Department's Public Safety and Security Division's Badging Office. Contractor must make arrangements with the City to have each Contract Worker proceed to the Badging Office for processing. The Badging Office will not issue a SIDA badge until the Contract Worker passes a fingerprint-based criminal history background check (CHRC) required by federal law (49 C.F.R. § 1542.209) and § 4-22(C) of the Phoenix City Code and passes a security threat assessment as mandated by the TSA through a security directive (49 C.F.R. § 1542.303). The Contract Worker shall comply with all requirements of and furnish all information requested by the Badging Office. Contractor shall pay for all fees associated with SIDA badging process, unless otherwise provided in the Scope of Work. Fees will be assessed according to § 4-22(D) of the Phoenix City Code. Current badging procedures and fees are available for review at https://www.skyharbor.com/airport-business/security-badging/badging-information.

   As used in this Section, "restricted area" means the secured area and SIDA area of the Airport. "Secured area" means the part of the Airport in which certain federal security measures are implemented and where airlines enplane and deplane passengers and load baggage. "SIDA area" means the secured area and other areas designated by the Aviation Department, which include air operation areas, ground transportation areas, and the Rental Car Center security doors. "Sterile area" means the part of the Airport that provides passengers access to board aircraft and is controlled by the TSA or the airline by screening of persons and property. See § 4-22 of the Phoenix City Code and Rules 05-01 and 05-09 of the Aviation Department Rules and Regulations for a complete definition of the foregoing terms.

4. **RISK-BASED BACKGROUND CHECK PROCESS:** The City has established two levels of risk for Contract Worker background checks: standard risk and maximum risk. If the Scope of Work changes, the City may change the level of risk, which may require Contractor conduct additional investigations and incur additional costs in order to process a background check and obtain the required airport security badge. Contract Workers who receive a SIDA badge are exempt from a standard and maximum risk background check and will be required to pass Criminal History Records Checks (CHRC) and Security Threat Assessments (STA).

   A MAXIMUM RISK BACKGROUND CHECK is required for all non-exempt Contract Workers performing work under this Contract.

As used in this Section, “background check” means the fact-gathering process described in City of Phoenix A.R. 4.45 that is conducted to obtain information regarding a Contract Worker’s criminal history, driving history, certifications, and other matters that may affect the Contract Worker’s ability or fitness to perform work under this Contract.

4.1. Before any work is performed under this Contract, Contractor shall provide the City with a list of its Contract Workers.

4.2. If any dispute arises related to a background check process or criminal history check information, then Contractor and the affected Contract Worker will resolve the dispute. The City will not get involved in resolving any such dispute.

4.3. In making the determination whether information in a background check renders the Contract Worker disqualified, Contractor should be guided by the following principles and guidelines:

4.3.1. Disqualification should not be based solely on a criminal conviction, unless the conviction related to performance under this Contract.

4.3.2. Arrests that did not result in a conviction being entered or charges being filed may not be considered.

4.3.3. Not all criminal convictions or other negative information obtained in a background check will disqualify a Contract Worker from working under this Contract.

4.3.4. Contractor must evaluate the relevance of the information to the work the Contract Worker will perform under this Contract.

4.3.5. Contractor must consider the following factors in determining whether negative background information disqualifies a Contract Worker:

- Duties of the position
- Time, nature, and number of negative events and convictions
- Attempts and extent of rehabilitation efforts
- The relation between the duties of the position and the nature of the crime committed

4.4. The analysis of whether any information in a background check is a potentially disqualifying factor involves looking at the requirements of the Contract, the Scope of Work, where the work will be performed, the need for access to restricted areas, and the type of persons or places the Contract Worker will encounter. Contractor should review the background check results and determine whether the nature of the conviction or crime reported would create a risk to the City based on the Contract's requirements.

4.4.1. For a Contract Worker requiring a standard risk background check, potentially disqualifying convictions include a record of theft, identity theft, computer fraud or abuse, burglary, arson, crimes against property, violent crimes, or other crimes involving dishonesty, or embezzlement.

4.4.2. For a Contract Worker requiring a maximum risk background check, potentially disqualifying convictions include a record of child molestation, assault, sexual assault, crimes against a person, public indecency, drug offenses, forgery, theft, burglary, arson, crimes against property, violent crimes, crimes for financial gain, identity theft, computer fraud or abuse, and embezzlement.

4.5. If a background check shows that the disposition of an arrest is unknown, then Contractor must determine the disposition of the arrest.

4.6. Contractor will obtain a Contract Worker disclosure from each Contract Worker who will perform work under this Contract. Contractor will provide the Contract Worker disclosures to the City upon request. "Contract Worker disclosure" means an affidavit by a Contract Worker disclosing his or her prior criminal record. The Contract Worker disclosure must list all criminal convictions, including the nature of the crime, the date of the conviction, and the location where the crime and conviction occurred. The Contract Worker disclosure also grants to the City the right to review the background check results. (City of Phoenix A.R. 4.45)

4.7. In a standard risk background check, Contractor must review the results of the background check and decide if a Contract Worker should be disqualified for work under this Contract. Contractor must engage in whatever due diligence is necessary to make the decision on whether to disqualify a Contract Worker. After Contractor has made its decisions, a list of names of qualified Contract Workers will be provided to the City.

4.9. In a maximum risk background check, Contractor must conduct the same review as in a standard risk background check. However, when submitting its list of qualified Contract Workers, Contractor must also submit the results of the background checks to the City for review. After its review, the City will either approve or deny each Contract Worker.

4.9.1. If the City approves a Contract Worker, then the City will notify Contractor of that fact and the Aviation Department will issue the appropriate airport security badge to the Contract Worker.

4.9.2. If the City denies a Contract Worker, then the City will notify Contractor of that fact and Contractor will reevaluate the Contract Worker to determine whether the person should be disqualified. If Contractor believes there are extenuating circumstances that suggest that the Contract Worker should not be disqualified, then Contractor will discuss those circumstances with the City. The City will review the matter and its decision on disqualification is final.

4.9.3. The City may set up a secure folder or drop box for confidential materials related to maximum risk background checks. The City will not keep records related to maximum risk background checks after they are reviewed.

4.10. If Contractor is a sole proprietor, Contractor must submit to the City a copy of his or her own background check and a background check for all business partners, member, and employees that will work under this Contract and for whom the background check requirements of City of Phoenix A.R. 4.45 apply.

4.11. Contractor shall determine whether a Contract Worker is disqualified from performing work under this Contract.

5. STANDARD RISK BACKGROUND CHECK: A standard risk background check must be conducted for the term of this Contract or five (5) years, whichever is shorter. Contractor shall conduct a standard risk background check on all Contract Workers whose work under this Contract requires:

- An airport security badge or key for access to City facilities,
- Access to sensitive information, confidential records, personal identifying information, or restricted City information, or
- Unescorted access to City facilities during normal and non-business hours.

"Personal identifying information" is defined by City of Phoenix A.R. 4.45.

5.1. Scope of the Standard Risk Background Check: The standard risk background check conducted by Contractor must be based on the real identity and legal name of the Contract Worker and include felony and misdemeanor records checks from any county in the United States, the state of Arizona, and any other jurisdiction where the Contractor Worker has lived at any time in the last seven (7) years.

6. MAXIMUM RISK BACKGROUND CHECK: A maximum risk background check must be conducted for the term of this Contract or five (5) years, whichever is shorter. Contractor shall conduct a maximum risk background check on all Contract Workers whose work under this Contract requires:

- Working directly with a vulnerable adult or child under age 18,
- Any responsibility for the receipt of payment of City funds or control of inventories, assets, or records that are at risk of misappropriation,
- Unescorted access to City data centers, money rooms, high-valve equipment rooms,
- Access to a private residence,
- Access to Homeland Defense Bureau-identified critical infrastructure sites or facilities, or
- Responsibility or access to City-identified critical infrastructure sites, City networks or data, cyber/IT/network assets, digital or cyber assets, workstations, or servers, by either remote or direct access.

6.1. Scope of the Maximum Risk Background Check: The maximum risk background check conducted by Contractor must include the search criteria conducted under a standard risk background check in addition to a search for all felony and misdemeanor convictions (not including traffic or parking violations), a sex offender check, and a search for all outstanding warrants. Based on the Scope of Work, Contractor shall also conduct a credit check (for cash handling, accounting, and compliance positions only), driving records check (for driving positions only), and fingerprint verification when the Contract Worker is working directly with a child under age 18 or a vulnerable adult or the work under the Contract will take the Contract Worker to a criminal justice information system (CJIS) location.

Maximum risk background checks are valid for the term of this Contract or three (3) years, whichever is shorter.

6.2. Maximum Risk Background Check for Child Care Staff Members: If the Scope of Work of this Contract involves work as a child care staff member, then Contractor will conduct a maximum risk background check.

6.4. Criminal Justice Information System (CJIS) Maximum Risk Background Check: If the Scope of Work of this Contract requires unescorted access to a CJIS location or if Contractor will have access to a CJIS infrastructure or information, then a CJIS maximum risk background check will be conducted, reviewed, and approved by the Phoenix Police Department or the Arizona Department of Public Safety.

6.5. Maximum Risk Background Check for Children or Vulnerable Adults: If the Scope of Work of this Contract involves work with a child under age 18 or a vulnerable adult, then Contractor will conduct a maximum risk background check.

As used in this Section, "vulnerable adult" means an individual who is 18 years of age or older who is unable to protect himself or herself from abuse, neglect, or exploitation by others because of a mental or physical impairment. (A.R.S. § 13-3623(F)(6) and City of Phoenix A.R. 4.45)

7. AIRPORT SECURITY BADGE HANDLING PROCEDURES: Contractor will comply with the following airport security badge handling procedures:

7.1. Key Access Procedures: If a Contract Worker requires keyed access to enter a City facility, then a separate key will be issued and Contractor must complete a return form and submit it to the City for each key issued.

7.2. Stolen or Lost Badges or Keys: Contractor shall immediately report any lost or stolen airport security badge or key to the City. A new airport security badge application or key issue form must be completed and submitted along with payment of the applicable fee prior to issuance of a new airport security badge or key

7.3. Return of Badges or Keys: All airport security badges and keys are the property of the City and must be returned to the Badging Office within one (1) business day after the Contract Worker's access to a City facility is no longer required under this Contract. Contractor shall collect a Contract Worker's airport security badge and all keys (1) when the Contract Worker's employment is terminated, (2) when the Contract Worker's services are no longer required at a City facility, or (3) when this Contract terminates, is cancelled, or expires, whichever occurs first.

7.4. Employee Identification and Access: Contract Workers must have an airport security badge and some form of verifiable company identification in their possession at all times while working under this Contract, unless otherwise provided in the Scope of Work. Contract Workers are strictly prohibited from entering any area of the Airport that is not authorized by the airport security badge or key issued to them by the Badging Office.

The Aviation Department will determine who will have access to the Airport. Contract Workers access authority is only valid during their scheduled hours. Contractor shall provide the City with updates and changes in personnel as they occur.

7.5. Badge Fees: Contractor shall pay the airport security badge fees set forth in § 4-11(D) of the Phoenix City Code.

8. CONTRACTOR'S BREACH: Contractor agrees that the access control, airport security badge, and key requirements in this Section are necessary to preserve and protect public health, safety, and welfare. Therefore, Contractor shall be deemed in immediate breach of this Section upon the occurrence of any of the following:

- A Contract Worker gains access to a City facility or a restricted or secured area of the Airport without the proper airport security badge or key
- A Contract Worker uses another person's airport security badge or key to gain or attempt to gain access to a City facility or a restricted or secured area of the Airport
- A Contract Worker begins work under this Contract without passing the appropriate Background Screening and being issued the proper airport security badge or key
- A Contract Worker or Contractor submits false, incomplete, or misleading Background Screening information or submits any false, incomplete, or misleading information in an attempt to improperly obtain an airport security badge or key
- Contractor fails to collect and timely return a Contract Worker's airport security badge or key to the City within three days of the (1) date the Contract Worker's employment terminates, (2) the date the Contract Worker is assignment to another City facility, or (3) when this Contract terminates, is cancelled, or expires, whichever occurs first.

9. CONTRACTOR CERTIFICATION: Contractor certifies to the City that Contractor has read the foregoing Background Screening requirements and that all Background Screening information Contractor furnished to the City is accurate, complete, and current. Contractor further certifies to the City that Contractor has satisfied all Background Screening requirements and verified the legal worker status of each Contract Worker as required under this Section.

10. CONFIDENTIALITY: "Confidential Information" means all non-public, confidential, sensitive, or proprietary information disclosed or made available by City to Contractor or its affiliates, employees, contractors, partners, or agents (collectively "Recipient"), whether disclosed before or after the Effective Date, whether disclosed orally, in writing, or via permitted electronic access, and whether or not marked, designated, or otherwise identified as confidential. Confidential Information includes, but is not limited to: user contents, electronic data, meta data, employment data, network configurations, information security practices, business operations, strategic plans, financial accounts, personally identifiable information, protected health information, protected criminal justice information, and any other information that by the nature and circumstance of the disclosure should be deemed confidential. Confidential Information does not include this document or information that: (a) is now or subsequently becomes generally available to the public through no wrongful act or omission of Recipient; (b) Recipient can demonstrate by its written records to lawfully have had in its possession prior to receiving such information from the City; (c) Recipient can demonstrate by its written records to have been independently developed by Recipient without direct or indirect use of any Confidential Information; (d) Recipient lawfully obtains from a third party who has the right to transfer or disclose it; or (e) the City has approved in writing for disclosure.

Recipient shall: (a) protect and safeguard Confidential Information with at least the same degree of care as Recipient would protect its own Confidential Information, but in no event with less than a commercially reasonable degree of care, such as ensuring data is encrypted in transit and at rest and maintaining appropriate technical and organizational measures in performing the Services under the Agreement; (b) not use Confidential Information, or permit it to be accessed or used, for any purpose other than in accordance with the Agreement; (c) not use Confidential Information, or permit it to be accessed or used, in any manner that would constitute a violation of law, including without limitation export control and data privacy laws; and (d) not disclose Confidential Information except to the minimum number of recipients who have a need to know and who have been informed of and agree to abide by confidentiality obligations that are no less restrictive than the terms of this Agreement. If Recipient is required by law or court order to disclose any Confidential Information, Recipient will first give written notice to the City and provide the City with a meaningful opportunity to seek a protective order or limit disclosure.

Upon the City's written request or expiration of this Agreement, whichever is earlier, Recipient shall, at no additional costs to the City, promptly return or destroy all Confidential Information belonging to the City that Recipient has in its possession or control. After return or destruction of the Confidential Information, Recipient shall certify in writing as to its compliance with this paragraph.

If applicable, Contractor agrees to comply with all City information technology policies and security standards, as may be updated from time to time, when accessing City networks and computerized systems whether onsite or remotely.

In addition to, and not in lieu of, all other rights and remedies available to the City, Contractor will defend, indemnify, and hold the City harmless against all losses, claims, costs, attorneys' fees, damages or proceedings arising out of Contractor's breach of this Section (Confidentiality). Contractor's obligations pursuant to this Section (Confidentiality) shall not be subject to any limits of liability or exclusions as may be stated elsewhere in the Agreement.

A violation of this Section shall be deemed to cause irreparable harm that justifies injunctive relief in court. A violation of this Section may at the City's discretion result in immediate termination of this Agreement without notice. The obligations of Contractor under this Section shall survive the termination of this Agreement.

11. DATA PROTECTION: The parties agree this Section shall apply to the City's Confidential Information and all categories of legally protected personally identifiable information (collectively "PII") that Contractor processes pursuant to the Agreement. "Personally identifiable information" is defined as in the Federal Privacy Council's Glossary available at: https://www.fpc.gov/resources/glossary/.

As between the parties, the City is the data controller and owner of PII and Contractor is a data processor. In this Section, the term "process," "processing," or its other variants shall mean: an operation or set of operations which is performed on PII, whether or not by automated means, including without limitation: collection, recording, copying, analyzing, caching, organizing, structuring, storage, adaptation, alteration, retrieval, transmission, dissemination, alignment, combination, restriction, erasure, or destruction.

11.1. When Contractor processes PII pursuant to the Agreement, Contractor shall, at no additional cost to the City:

11.1.1. process PII only within the United States and only in accordance with the Agreement and not for Contractor's own purposes, including product research, product development, marketing, or commercial data mining, even if the City's data has been aggregated, anonymized, or pseudonymized;

11.1.2. implement and maintain appropriate technical and organizational measures to protect PII against unauthorized or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure, including at a minimum, and as applicable, those measures specified by the National Institute of Standards and Technology (NIST) SP800-53; A.R.S. § 18-552 (Notification of Security System Breaches); A.R.S. § 44-7601 (Discard and Disposal of Personal Identifying Information Records); Health

Information Technology for Economic and Clinical Health (HITECH) Act; Payment Card Industry Data Security Standards; and good industry practice; (When considering what measures are appropriate and in line with good industry practice, Contractor shall keep abreast of current regulatory trends in data security and the state of technological development to ensure a level of security appropriate to the nature of the data to be protected and the harm that might result from such unauthorized or unlawful processing or accidental loss, destruction, damage, theft, alteration or disclosure. At minimum, Contractor will timely remediate any vulnerabilities found within its network that are rated medium or more critical by the Common Vulnerability Scoring System (CVSS); however, Contractor must remediate vulnerabilities that are rated critical within 14 days and vulnerabilities that are rated high within 30 days. If requested by the City, Contractor shall promptly provide a written description of the technical and organizational methods it employs for processing PII.)

11.1.3. not subcontract any processing of PII to any third party (including affiliates, group companies or sub-contractors) without the prior written consent of the City; and Contractor shall remain fully liable to the City for any processing of PII conducted by a sub-processor appointed by Contractor;

11.1.4. as applicable, implement and maintain appropriate policies and procedures to manage payment card service providers with whom Contractor shares sensitive financial information or cardholder data; and provide the City with a Qualified Security Assessor Attestation of Compliance for Payment Card Industry Data Security Standards on an annual basis, but no later than within 30 days of attestation report completion;

11.1.5. take reasonable steps to ensure the competence and reliability of Contractor’s personnel or sub-processor who have access to the PII, including verifications and background checks appropriate to the security level required for such data access;

11.1.6. maintain written records of all information reasonably necessary to demonstrate Contractor’s compliance with this Agreement and applicable laws;

11.1.7. allow the City or its authorized agents to conduct audit inspection during the term of the Agreement, but no more than once per year, which may include providing access to the premises, documents, resources, personnel Contractor or Contractor's sub-contractors use in connection with the Services; provided however, the City may at its sole discretion accept a qualified and industry recognized independent third-party assessment report or certification (such as SSAE 18 SOC 2 or ISO/IEC 27001) provided by Contractor at no cost to the City in lieu of the audit inspection rights of this Section;

11.1.8. If Contractor becomes aware of any actual or potential data breach (each an "Incident") arising from Contractor's processing obligations pursuant to the Agreement, Contractor shall notify the City at SOC@phoenix.gov without undue delay within 48 hours; and:

11.1.9. provide the City with a detailed description of the Incident, the type of data that was the subject of the Incident, and the identity of each affected person as soon as such information can be collected or otherwise becomes available;

11.1.10. take action immediately, at Contractor's own expense, to investigate the Incident and to identify, prevent, and mitigate the effects of the Incident and to carry out any recovery or other action necessary to remedy the Incident;

11.1.11. cooperate with the City in investigating the occurrence, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable laws or as otherwise required by the City; and

11.1.12. not directly contact any individuals who may be impacted by the Incident or release or publish any filing, communication, notice, press release, or report concerning the Incident without the City's prior written approval (except where required to do so by applicable laws).

11.1.13. In addition to, and not in lieu of, all other rights and remedies available to the City, Contractor will defend, indemnify, and hold the City harmless against all losses, claims, costs, attorneys' fees, damages or proceedings arising out of Contractor's breach of this Section (Data Protection).

11.1.14. Contractor's obligations pursuant to this Section (Data Protection) shall not be subject to any limits of liability or exclusions as may be stated elsewhere in the Agreement.

A violation of this Section shall be deemed to cause irreparable harm that justifies injunctive relief in court. A violation of this Section may at the City's discretion result in immediate termination of this Agreement without notice. The obligations of Contractor under this Section shall survive the termination of this Agreement.

12. **SECURITY INQUIRIES**: Contractor acknowledges that all of the employees that it provides pursuant to this Contract shall, at Contractor's expense, be subject to background and security checks and screening at the request of the City. Contractor shall perform all such security inquiries and shall make the results available to the City for all employees considered for performing work (including supervision and oversight) under this Contract. City may make further security inquiries. Whether or not further security inquiries are made by the City, City may, at its sole, absolute and unfettered discretion, accept or reject any or all of the employees proposed by the Contractor for performing work under this Contract. Employees rejected by the City for performing services under this Contract may still be engaged by Contractor for other work not involving the City. An employee rejected for work under this Contract shall not be proposed to perform work under other City contracts or engagements without the City's prior approval.