Exhibit D – Security Access Controls

Security, Access, Controls and Badging Information – City of Phoenix Public Transit Department

Section 1: Introduction

The City has an obligation to protect employees and the visiting public, preserve the availability of assets and ensure the continued delivery of services effectively, safely, and cost-efficiently. Identification cards (ID Cards) and Electronic Access Badges help the City accomplish all of these goals. With the addition of policies for Intrusion Detection Systems (Alarms) and issuing physical keys, this document serves as the central document related to Security, Access Controls and Badging Information for the Public Transit Department.

Section 2: The Policy

2.1 – Introduction

Administration Regulation (AR) 4.44 and 4.45 were revised and adopted by the City of Phoenix on September 1, 2018. These regulations provide most of the policy guidelines referred to in this document. AR 4.44 provides guidelines for assessing risk and managing access to City facilities and City assets. AR 4.45 governs Contract Worker background screening.

A. Standard Risk Background Check

1. A standard risk background check will be conducted for the contract term or 5 years, whichever is shorter when the contract worker's work assignment will result in any of the following:
   • Requires a badge or key for access to City facilities; or
   • Access to sensitive, confidential records, Personal Identifying Information or restricted City information; or
   • Unescorted access to City facilities during normal and non-business hours.

2. Standard Risk level will require a background check based on real identity/legal name and include felony and misdemeanor records checks from any county in the United States, the State of Arizona, plus any other jurisdiction where the contract worker has lived at any time in the last seven years.

B. Maximum Risk Background Check

1. A maximum risk background check will include all search criteria performed under a standard background check.

2. A maximum risk background check will be conducted for the contract term or 5 years, whichever is shorter, except as noted for child care or CJIS related contracts when the contract worker's work assignment will result in any of the following:
   • Work directly with vulnerable adults or children (under the age of 18) (see definitions).
   • Responsibility for the receipt or 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, or high-value equipment rooms.
   • Access to private residences.

- Access to Homeland Defense Bureau identified critical infrastructure sites/facilities.
- Responsibility or access to City identified critical infrastructure sites, City networks or data, cyber/IT/Network assets, digital or cyber assets, workstations or servers (either remote access (VPN) or direct access).

3. <u>Maximum Risk Background Check Must Include:</u>
   - Criminal record, conviction of a misdemeanor (not including traffic or parking violation) or felony.
   - Sexual offender search.
   - All outstanding warrants.

4. <u>Maximum Risk Background Check for Child Care Staff Member Must Include:</u>
   - A Federal Bureau of Investigation fingerprint check using Next Generation Identification.
   - A search of the National Crime Information Center's National Sex Offender Registry.
   - A search of the following registries, repositories, or databases in the State where the child care staff member resides and each State where such staff member resided during the last five years:
     (i) State criminal registry or repository, with the use of fingerprints being:
        (A) Required in the State where the staff member resides;
        (B) Optional in other States;
     (ii) State sex offender registry or repository; and
     (iii) State-based child abuse and neglect registry and database.

5. <u>Criminal Justice Information System (CJIS) Background:</u>
   - The background checks for this level will consist of a local, state and national fingerprint-based record check to be conducted by the Phoenix Police Department or the Arizona Department of Public Safety.
   - An additional CJIS check will be performed if unescorted access is required to an identified CJIS location or if the contractor will have access to CJIS infrastructure or information.

6. <u>Additional Required Background Check Based on Work Scope:</u>
   - Credit Check (for cash handling, accounting, and compliance positions only).
   - Driving records (for driving positions only).
   - Fingerprint verification (when contract worker is working directly with children or vulnerable adults or job takes the individual to a CJIS location).

7. <u>Legal Requirements</u>: Contract workers who work directly with children or vulnerable adults are subject to fingerprint verification.
   - Contract worker maximum or Criminal Justice Information System (CJIS) background check will be valid for whichever is shorter, the contract term or three years for healthcare or nursing care related contracts

2.2 – Roles and Responsibilities

1. Monitoring of the Access Control and Security Systems is the responsibility of the Police Department – Central Monitoring Station (CMS).

2. The Public Works Department Alarm Services Section is responsible for specifying, implementing and maintaining the City's badge access system in accordance with accepted industry standards and best practices. Card Access Control Systems must sufficiently meet current and emerging credible threats and standards.

3. The Public Works Department Badge Imaging Office and Public Transit Department Facilities Division control the production, issuance, and accountability of access badges.

4. Periodic reviews of programmed access, clearance codes and inactive badges must be performed by the contractor, Facilities Division, and the Badge Imaging Office to ensure current, valid and relevant access into City facilities.

2.3 – Badge Use and Conditions of Use

Access badges issued by the City of Phoenix remain the property of the City and should be collected and returned to the Facilities Division once no longer required.

While on City property, badge holders must visibly display badges and present government identification upon request of management, security personnel, or law enforcement.

Contract Workers with authorized access are entitled to have the City of Phoenix Contractor Badge and their company identification badge in their possession while on

City property. Only one City access badge is assigned and active for a contract worker. Having more than one active badge assigned to the same person can pose a serious potential security breach. It is important that the contractor and the Facilities Division track and ensure their workers are using the appropriate badge.

Access badges are not transferable. City access may only be used by the person it was issued to. No access may be loaned or borrowed.

All City badge holders are responsible for appropriate care and control of their access badge in accordance with the City of Phoenix Administrative Regulations and contract policies. Badge holders must immediately notify the contractor and the Facilities Division upon noticing their badge is lost, stolen, missing or damaged.

Permanent photo access badges must be picked up personally by the recipient from the Facilities Division Badge Office, during posted office hours, and signed for on the badge application at the Facilities Division Badge Office location.

No one may circumvent, bypass or otherwise render ineffective any City badge access devices. This includes badge readers, locking mechanisms, door sensors, etc. Any intentional attempts to do so shall be regarded as a criminal act.

2.4. – Protection of Information

Personal information for badging purposes is used to issue employees and contract worker access badges and for contact purposes in case of an emergency. The Facilities Division Badge Office and the Badge Imaging Office staff are entrusted to ensure confidential information remains confidential.

Badge access information may not be divulged except in compliance with the City of Phoenix policies and procedures or directives. Any requests for confidential information should be forwarded through the appropriate channels. The information contained in the security system(s) database must not be used for non-security purposes including, but not limited to, time, attendance, and data gathering for disciplinary purposes.

2.5 – Consequences

Violations of this Policy may be subject to disciplinary action at the discretion of the department.

Section 3: Procedures

3.1 – Background Screening Review Process

There are specific requirements that must be completed prior to the Public Works Department Badge Imaging Office and the Public Transit Department Facilities Division Badge Office issuing an Access Badge. Both badging offices will require Facilities Division Management Assistant II signature, contractor representative signature, City contract manager signature, employees and contract workers to complete badge documentation and submit information in order to create a badge and for validation purposes.

Contractor badges may only be issued to contract workers if:
- A business need exists for the worker to have unescorted electronic access to common and secure areas of City facilities;
- A background check has been conducted
  - Level of Access (Standard, Maximum, and Maximum Criminal Justice Information System (CJIS)) is determined by the Facilities Division Management Assistant II in conjunction with City Risk Assessment Guide.
  - The contractor shall be responsible for determining whether a contract worker is qualified to perform work or disqualified from performing work for the City under the terms of the contract for standard, maximum and CJIS risk level background checks.
  - For standard level background check requirements, the contractor will provide a list of "eligible contract workers" on the contractor's company letterhead, to the Facilities Division Management Assistant II.
  - The contractor will provide a complete background check report for the maximum level background check to the Facilities Division Management

> Assistant II (MAII). The MAII will review and approve/disapprove maximum risk background check results.

> ➢ Maximum risk background check results are to be submitted to the MAII in a sealed, confidential envelope, at a minimum of 5 business days before work is to begin.

> ➢ The MAII will secure al/'l maximum risk background check results in a locked file cabinet until the review is complete.

> ➢ The MAII will discard of the maximum risk background check results in the confidential secured bin that is picked up by an offsite secured shredding company.

> ➢ The contract worker is to work directly with the contractor, not the City, to resolve any disputes related to the background check process and/or outstanding Criminal History Records Check Information.

> ➢ CJIS risk background will consist of local, state, and national fingerprint-based record check to be conducted by the Phoenix Police Department or the Arizona Department of Public Safety.

> ➢ All contractors, except **employees** of 302 Building tenants, must pay a $55 badge fee before issuance of an access badge.

> ➢ Please note that subcontractors, whether of a tenant or primary contractor, will be charged the $55 fee, no exceptions.

- Access badges will not be issued if background checks are incomplete, badge applications are incomplete, photo identification is not presented at the time of issuance, background check has been denied, badging fee not paid, or sufficient time not allowed for review.

- Individuals must come in for issuance of an Access Badge within 30 days from date of maximum risk background check results or standard risk "eligible contractor worker" list.

3.2 – Company Responsibility for Contractors

Each Contract company shall designate a primary and secondary representative who will work directly with their Designated Authorized Signer to have their contract worker(s) complete the necessary steps to perform services. The Contract companies representative(s) are responsible for complying with all requirements associated with conducting business and performing services for the City of Phoenix. Contract companies must ensure their contract workers complete the appropriate paperwork in a timely manner and any supporting documentation requested by their Designated Authorized Signer.

The Designated Authorized Signers are responsible for authorizing and approving the City of Phoenix Badge Data Form. In addition, the Designated Authorized Signers are responsible for making access related notifications to their Public Transit Department Badge Office staff regarding changes in status for contract workers such as lost and stolen badges and issues where replacement badges are required to ensure they are deactivated in the system properly. The Badge Office staff will require that each Contract Manager or Tenant Representative Authorized Signer communicate badge, access, and background check information to the Contract companies representative(s) to ensure consistency and that processes are followed properly.

3.3 – AR-Applicable Contracts: Background Check Process

The following regulations apply to all contracts that contain background screening language as it was approved by the Law Department.

Contractors perform a variety of work for the City. The type of work performed and the work environment influence the need for three levels of risk, each of which requires a background check. The first level involve circumstances where background checks are required and performed by the contractor and the second level where the background check is performed by the contractor, but reviewed by City Departments. The third level the Police Department Local Agency Security Officer (LASO) must review and approve all CJIS background checks.

Contractors must have workers complete and sign a copy of the Contract Worker Disclosure Form before the background check is conducted.

The Contract Worker Disclosure Form will provide an opportunity for the contract worker to list any and all criminal convictions and grant the City the right to review the background check results.

3.4 – AR-Applicable Contracts: Evaluating Results

The contractor shall be responsible for determining whether a contract worker is disqualified from performing work for the City under the terms of the contract for standard level background checks.

For standard-level background screening, the contractor will provide the contracting department a memo indicating the types of screenings performed and that the contract worker passed those screenings (See Section 2.6).

For maximum and CJIS-level background screening, the contracting department will review and approve the background check provided by the contractor. The department will prepare a memo to be placed in the contract file that indicates the results of each worker's background check.
The contract worker is to work directly with the contractor (not the City) to resolve any disputes related to the background check process and/or any outstanding Criminal History Records Check information.

In making the determination of whether information contained in the results of the background checks constitute grounds for disqualification of a contract worker, the contractor and contracting department should be guided by these principles and guidelines:

- Disqualification decisions should not be based solely on a criminal conviction, unless the conviction is related to performance under the contract. Arrests that did not result in a conviction or have not been charged may not be considered when determining whether a contract employee is disqualified.

- Not all criminal convictions or other negative information obtained in the background screening process would prohibit an individual to work under the contract. Departments must evaluate the job relatedness of the information

received. To determine if a contract employee's background would be prohibitive for a specific contract, these factors should be analyzed:

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

The analysis of whether or not any particular item in a background check is a potentially disqualifying factor involves looking at what the contract work requires, where the work is done, the access to particular areas, and the type of people or places that the contract worker will encounter. Then the background results should be reviewed to determine whether the nature of the crime reported would create a risk to the City based on that person's background. An example of this analysis would be as follows:

Note: For a vendor who is contracting with the City requiring less screening but needing credentials (for example not needing access to City facilities but working on City assets) a minimum risk background check is required, there is no conviction that should disqualify a person for the work, since at this level, the contract worker does not have direct access to City facilities, does not come in contact with vulnerable people, does not have access to private property, and only has escorted access to City facilities. The only disqualifying factors would be if the contract worker did not meet the requirements of A.R.S. § 41-4401*Government Procurement; E-verify Requirement*.

For a person who is contracting for work requiring a standard risk background check, potentially disqualifying convictions could include a record of theft, burglary, arson, crimes against property, violent crimes, or other crimes involving dishonesty, or embezzlement.

For a person who is contracting for work requiring a maximum and CJIS risk background check, potentially disqualifying convictions could 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, and embezzlement.

If a contract worker has a criminal record that includes a disqualifying conviction, that person shall not be permitted to perform work for the City under the contract. If the records check indicates that the disposition of the criminal case is unknown, the contractor must determine the disposition.

3.5 – Badge Office Locations and Contacts

The Public Works Department Badge Imaging Office is located on the Mezzanine in the Calvin C. Goode Building. Employees and contractors without a valid parking pass may park in the 305 Garage (305 West Washington) or at a parking meter. Individuals will enter the building through the main lobby entrance and proceed to the single elevator located directly east of the main elevator banks. Employees and contractors are only to utilize this location upon prior approval from the Public Transit Department Facilities Division Badging staff.

Public Works Department
Badge Imaging Office
251 West Washington, Mezzanine
Phoenix, Arizona 85003
Monday – Friday
8 am to 12 pm, 1 pm to 4 pm
602-534-4611

The Public Transit Department has (3) three badge office locations. All information must be received by badging staff prior to individuals coming in for issuance of an Access Badge.

Public Transit Headquarters
302 North 1st Avenue, Ste. 900
Phoenix, Arizona 85004
602-495-5914

West Transit Facility
405 North 79th Avenue
Phoenix, Arizona 85043
602-534-9121

2225 West Lower Buckeye
Phoenix, Arizona 85009
602-495-7690

3.6 – Fees and Payment Info
Payment must be submitted to badging staff with submission of application, unless prior arrangements have been made with the Facilities Division Management Assistant II.

Initial Badge Fee………………………………………………………$55.00
Renewal Badge Fee……………………………………………………$55.00
Lost or Damaged Replacement Badge Fee……………………………$55.00
Stolen Replacement Badge Fee…………………….PD Department Report – No Charge
(Report # is required on the Badge Data Form, if individual does not have proof of report $55 will be charged)

3.7 – How Access Badges Work
The proximity access badges used by the City of Phoenix have a microchip embedded inside them. The badge holder is required to present their issued badge to the card readers only in the areas they are authorized. Presenting badges to card readers that the individual does not have approved access to will trigger "denied wrong area" alarm activation to the Central Monitoring Station.

3.8 – Badge Number
The access badge number is the last four to six digit number printed on the back of the badge in the lower right corner.

3.9 – Authorization for Access

Each Designated Authorized Signer shall establish an Access Authorized Signer List. The list shall be maintained by the Designated Authorized Signer and contain the name and signatures of individuals who have been given the authority to approve access, along with a description of the areas for which they are allowed to approve access. Signers should be at the highest possible level based on the level of security needed for each area.

The number of people each department authorizes to approve access should be limited to the fewest number needed to efficiently process requests. The Access Authorized Signer List must be kept current and on file with the appropriate badging and/or security office.

Authorization to grant employees and contract workers access shall be documented by the requesting department prior to the issuance of a badge, key, or PIN code. Documentation shall include, but is not limited to, the following:
- Employee's or contractor's true and legal name;
- Location and times of access needed;
- The reason for access to each area;
- Approval signature of Contract Company Authorized Signer; and
- Approval signature from the Designated Authorized Signer.

Section 4: Enrollment

4.1 – Identity Verification

It is imperative that photo identification be shown to Badge Office staff when a person has their photo taken for a badge. The integrity of the City's identification system relies on this procedure. Government-issued photo identification is the most reliable.

Acceptable types include:
- Passport
- Citizenship Card
- Photo Health Card
- Driver's License
- Photo Firearms License
- Native/Immigration Status Card
- Permanent Resident Card
- Other acceptable form of government-issued ID

Badging staff will not take a photo and issue a badge without acceptable identification.

4.2 – Information Collection

The following steps must be followed by the Public Transit Department Badge Office when collecting information on a badge candidate:
- Ensure that the badge request form is fully completed and that all required information is written clearly on the form.
- Check photo identification to verify that the name on the form matches the name on the ID. If the person does not have photo identification, they will need to take the necessary steps to obtain an appropriate photo ID.
- Badging staff will ensure the appropriate badge type has been checked. This will determine the type of badge template to issue.

- Validate signature of the person who signed the badge application.
  Validate payment method and process

4.3 - Photo Capture
City access and identification badges are used in many sensitive applications, including access into restricted City facilities, senior and childcare facilities, critical infrastructure and private homes, so it is important that the best quality picture be captured and applied.

Below are some guidelines to help obtain the above result:
- Hats or head coverings are not allowed, except if worn for religious reasons. If the photo candidate is permitted a head covering, the facial features must be fully and clearly visible.
- The candidate's eyes must be open and clearly visible.
- Glasses, including those tinted with a prescription, may be worn as long as the eyes are clearly visible. Sunglasses are not permitted.
- Photos must show both edges of the face clearly.
- Photos must show a full front view of face and shoulders squared to the camera.
- A small section of space may be left above the top of the head and below the neckline to show proportion.
- The face and shoulder image must be centered in the photo.
- Smiling is always permitted; however, unusual or contorted expressions will not be permitted.

4.4 – Retain Photocopy of Badging Sheet
The Badge Office staff will retain a copy of each processed Badge Data Form as long as the badge holder is active and in good standing with the City.

Section 5: Verification
Before any badge is produced, employment or affiliation with the City must be verified. No badges are to be produced without this verification.

5.1 Requirements for Verification
For City employees, the following information would satisfy the requirements of verification:
- Established record in the Human Resources e-CHRIS database;
- Confirmation of City department name, division, and section;
- Government-issued photo ID;
- Badge access requirements including all City facilities;

For a contractor, the following information would satisfy the requirements of verification:
- Confirmation of affiliation with a City department, function, division or program;
- Confirmation of passed and approved background check process;
- City affiliation; issued photo ID;

Expected contract completion/end dateThe contract manager must provide the Badge Office staff with the required information. Where the required information is not available, the Badge Office will advise the worker of the information required and will

request that they return when all information requirements have been satisfied. All information must be entered on the City of Phoenix Badge Data Form for retention and future auditing purposes.

5.2 – Confirm Employment Data
As part of the confirmation process, all relevant information must be collected. Relevant information includes:

- Badge Holder's name;
- Department, Function, Division and/or Contract Company worked for;
- Position/Title;
- Home Address and Phone Number;
- Work Location and Phone Number;
- Year of birth;
- Last 4-digits of Social Security Number;
- Emergency contact; and
- Badge Holder's Signature and current date;

5.3 – Confirm Access Requirement
The last part of the verification process involves the determination and authorization of access needs. Access must be requested by the Designated Authorized Signer(s) on behalf of the worker. Requests must be submitted in writing to the Badge Imaging Office and/or noted on the Badge Request form for processing.

Section 6: Production and Distribution
6.1 – Verify New Record
The Badge Office staff will research the database prior to entering a badge to ensure that another record does not already exist. If another badge record already exists, the latest information from the Badge Data Form and recent photo should be used to update the existing record, not replace it.

6.2 – Badge Pick-Up
All access or identification badges must be signed for at the Badge Office. Access badges may not be picked up by a co-worker or family member, and should not be inter-office mailed directly to the recipient.

Prior to issuing an ID or access badge, the Badge Imaging Office will ensure that any temporary badges issued to the badge holder are returned. This procedure enables proper badge tracking and auditing from production to issuance by maintaining continuity of possession.

6.3 – Identity Verification

It is important that ID and access badges be issued to the intended holder. When a badge holder arrives to pick up a photo ID or access badge, verification of the correct recipient is done using the badge holder's government issued photo identification.

Section 7: Maintenance
ID/Access Badges and Keys issued by the City of Phoenix are considered City property. Designated Authorized Signers must ensure employees and contract workers protect and

take care of City assets. Badges and Keys must be returned immediately to their appropriate issuing department when no longer required. Penalties may be assessed to the contracting department and/or the Contractor for failure to return these items.

7.1 – Lost and Stolen Badges
Active lost badges pose a serious potential security breach, similar to a lost key. It is imperative that employees and contract workers immediately report the badge as lost or stolen.

7.1.1 – Reporting Lost or Stolen Badges
Employees and contract workers are responsible for <u>immediately</u> notifying their Designated Authorized Signers of any lost or stolen badges so they can be deactivated and the appropriate precautions taken. Designated Authorized Signers must establish a method for reporting lost and stolen badges during afterhours.

Employees are responsible for completing the following steps:
- Notify the Designated Authorized Signer immediately;
- Notify the Public Transit Department Badge Office;
- Complete a new Badge Data Form signed by the Designated Authorized Signer and/or designee; and
- Complete payment process (if applicable).

Contract Workers are responsible for completing the following steps:
- Notify the Contract Company he or she is employed with;
- Notify the Designated Authorized Signer and/or designee; and
- Complete a new Badge Data Form signed by the contract worker and the Designated Authorized Signer.

Departments shall require a police report be filed for any stolen badges.

7.1.2 – Found Badges
Often times, ID/Access badges are reported lost at first and are later found. Badge holders are prohibited from using a badge that has been reported as lost or stolen, unless the Badge Imaging Office notifies the department or employee otherwise.

When a deactivated badge has been found, the Designated Authorized Signer and/or the contracting department shall report these conditions to the Badge Imaging Office immediately. The Badge Imaging Office will verify the badge record information. If a new badge has been issued, the Designated Authorized Signer is required to return the

badge that was found to the Badge Imaging Office. If a new badge has not been issued, the Badge Imaging Office staff will validate the badge holder's record information and update the status. It is vital to be sure the badge is being activated for the correct person.

The badge should only be re-activated after ensuring that a replacement badge has not yet been made. If no new badge has been issued, the badge may be reactivated at the discretion of the Designated Authorized Signer and the Badge Imaging Office.

7.1.3 – Replacement

Lost and stolen badges will be replaced once a new badge application is completed and signed by the appropriate Designated Authorized Signer. In the case of lost badges, the employee, contractor and/or contract worker will be responsible for the current replacement cost. In the case of a stolen badge that has been reported to the Police Department, a replacement will be provided at no cost. A new Badge Application must be completed and approved, along with the Police Department Report number, before a replacement badge is issued.

7.2 – Damaged and Defective Badges

From time to time, the microchip inside an access badge will become inactive or fail. Sometimes a badge will be cracked or otherwise damaged, rendering the badge inoperable. Badges that have sustained cosmetic damage to the front of the card, such as scratching, or fading, should be replaced if the image on the front of the card is no longer legible from an appropriate distance.

A new Badge Application needs to be completed before the badge can be reissued. Defective badges may be replaced at no cost, if it is determined that the employee or contract worker did not cause the defect. Payment is expected at time of application.

7.3 – Name Change

Employees or contract workers requesting a name change from their existing City – issued access badge must complete a new Badge Application signed by the appropriate personnel and pay the replacement cost at time application is submitted. The old badge must be returned at the time the new badge is issued.

7.4 – New Photo

Personal appearance can change significantly over time, due to changes in weight, hair color, style, etc. The goal is to have the City electronic access badge look like the person that is represents for security and safety reasons. If a new badge is issued within 6 months of previous badge, a new photo is required.

If an employee and/or contract worker wishes to take a new photo due to the individual's change in appearance, that request must be initiated from the Designated Authorized Signer and/or the contract manager. A new Badge Data Form must be completed and submitted to the Public Transit Department Badge Office.

The badge holder will be required to make a payment in the amount of $55 at the time of issuance of the new badge.

7.5 – Separation in Service

When there is a separation in service from the City of Phoenix involving an employee, it is the responsibility of the supervisor to report the change in status immediately in writing to the Public Transit Department Badge Office. This will ensure the badge record is deactivated in a timely manner and eliminate security and safety risks involving the use of the City issued badge. Badges must be collected and returned to the Badge Office.

If the former City of Phoenix employee returns to perform services under a contract, it is the responsibility of the supervisor to follow the guidelines outlined in the contract.

If there is a separation in service where a contract worker is no longer employed with their company, the contract company is responsible for reporting the change in status immediately to the Designated Authorized Signer. If the former contract worker later returns to work for that same company it is the responsibility of the contract company to re-screen the worker.

7.6 – Extended Leave
Badge access privileges will be suspended for all badge holders who are on authorized extended leave. The supervisor or contract company is responsible for reporting change in status immediately to the Designated Authorized Signer.

All cancelled badges must be returned to the appropriate Badge Office.

7.8 – Expired Badges
Badges are only valid through the expiration date printed on the front of the Access badges. It is the responsibility of the badge holder to ensure they are in possession of a current and valid badge. A new badge application must be completed by the individual and signed by the appropriate personnel to replace an expired badge.

When expired badges are presented to card readers as an attempt to gain entry, alarm activation are generated in the Police Central Monitoring Station (CMS). This is a violation of badge holder responsibilities and may result in discipline.

7.9 – Adding Access to Badges
If a need develops for a badge holder to have additional access, the designated person may request the additional access via email to the Public Transit Department Facilities Division Management Assistant II.

Section 8: Badge Holder Responsibilities
8.1 – Badge Responsibility Agreement
Badge Holders shall read and sign a Badge Responsibility Agreement acknowledging their responsibilities related to safeguarding and caring for their city-issued badge. The information found in a Badge Responsibility Agreement may vary between departments

and/or location based on the level of security maintained in each area, but should include the badge holder responsibilities outlined in Section 8 of AR 4.44. Departments are responsible for maintaining Badge Responsibility Agreements for each badge holder.

8.2 – Representing the City of Phoenix
Badge holders should recognize that a City of Phoenix badge demonstrates affiliation with the City of Phoenix, and the actions of City employees and contractors are closely watched by members of the public. All badge holders must act legally, responsibly, and respectfully while wearing the badge.

8.3 – Guidelines
Guidelines for wearing the badge include, but are not limited to:
- While badge holders are conducting business and performing services at City facilities, ID/Access Badges must be worn at all times; displayed on the outer

- most garment and visible for immediate identification purposes.
- Badge holders must not loan, borrow or share badges, keys or PIN codes.
- The person to whom a key or badge has been issued shall be held responsible for its use until it has been properly returned to the appropriate Department or the Badge Imaging Office.
- Any person found to be in possession of an unauthorized key or badge shall be liable for its use and may be subject to disciplinary or legal action.
- Lost or stolen badges or keys must be reported immediately.
- If badges or keys are found, employees and contract workers must notify appropriate personnel.
- Badge holders must use their assigned access cards to gain entry into work areas that have card readers. Keys, when issued, should only be used in an emergency situation as it will cause alarms to be activated.
- Badge holders shall not tamper, interfere, compromise, modify or circumvent any security system, measures or procedures.
- Badge holders shall not allow persons without a badge to follow them into a restricted or controlled environment unless being escorted by a badged employee.
- Badge holders shall ensure doors are secure and never left open.
- Badge holders must take care to secure their badges and keys. They should never be left on an employee's desk or vehicle. Alarm PIN codes must be memorized and never posted for view.
- Badges and keys must be returned to appropriate personnel when no longer needed or upon the termination or transfer of an employee or contract worker.
- Badge holders may be charged for the cost of replacing badges or re-keying locks.
- Badge holders shall question the presence of persons without a badge and report infractions.
- Badge holders shall not duplicate badges and/or keys.
- Badge holders shall immediately report all alarm activations that occur in error.

8.4 – Violations

Employees may be subject to disciplinary action for violation of these policies and procedures.

For contractors, violations of this section, or any other section of this document, are punishable by temporary or permanent suspension from contracting with the City. Contract companies and their workers may be subject to other fines or consequences, depending on the severity of the infraction.

Section 9: Department Responsibilities

9.1 – Introduction

Designated Authorized Signers and contract managers shall be responsible for ensuring the City of Phoenix A.R.'s for Badge and Access Control and Contract Worker Background Check policies are followed by all employees and contractors. The City and contract managers must communicate the badge and access control and background check requirement needs to the appropriate Badge Office at least one week prior to start of new employees and the contractor's work assignment(s).

9.2 – Auditing and Process Reviews

Departments shall perform regular employee audits to ensure employees are in compliance with the Administrative Regulations, understand their responsibilities, and Designated Authorized Signer and/or designees are following the required procedures.

Departments shall perform regular contract worker disclosure audits and process review per prescribed citywide guidelines in conjunction with the implementation of Administrative Regulation 4.45. The City Auditor Department may also perform audits as it deems necessary.

As a part of contract monitoring, the contract manager shall establish procedures for controlling contractor badges and a process for reporting lost/stolen cards. The same care and level of authorization should be applied to badges for a contractor as is for an employee badge (see AR 4.44, section 3 through 4G). All requirements, policies, and procedures related to contractor badges shall be documented in the contract.

9.3 – Training
The Designated Authorized Signers are required to conduct an internal Security Badge and Access training and awareness session for employees and contract workers. The Public Works Department Badge Imaging Office is available to assist departments in developing and/or improving their training program.

Section 10: Special Circumstances
10.1 – Contract Company Extensions/Special Access Request
When a contract is extended beyond the original end date of the contract, the department or division must contact the Badge Office. The department needs to ensure any contract workers who continue to work after the original expiration date of the contract will continue to have access. If contractors need additional access, or have a special access request, they are encouraged to contact the Badge Office.

10.2 – Working for Multiple City Departments/Multiple Contracts
Contract workers may be employed by multiple contract companies conducting business and performing services for the City of Phoenix. Contractors may be awarded multiple City contracts and perform services on behalf of multiple City departments. It is important for each City department to do their due diligence to ensure a proper background check has been conducted for contract workers according to the area and facility(s) assigned. This will ensure appropriate precautions have been considered to mitigate risk and liability for the City.

10.3 – Secondary Access Media
There are times when contract workers are employed by multiple companies doing business with the City of Phoenix and will require multiple badges. The Designated Authorized Signer must notify the appropriate Badge Imaging Office of the Contract company names, contract numbers and expiration dates, and determine the appropriate level(s) of access based on the areas and facilities associated with the duties performed by the contract worker. Contract workers must safeguard all issued media and follow all guidelines outlined in this policy.

10.4 – Access for Other Government Agencies

A non-City of Phoenix Government agency requesting an ID/Access Badge for City facilities/sites may, at the discretion of the Designated Authorized Signer waive certain fees outlined in the Fee Schedule.

Section 11: Intrusion Detection (Alarm) Systems

11.1 – Introduction

An Intrusion Detection System is an important device in protecting City of Phoenix facilities. Many City facilities are equipped with Intrusion Detection Systems (burglar alarm) and other specialized system devices to protect people, facilities, and assets.

These systems are electronic and can be controlled through a low voltage hard-wire or wireless transmitters and receivers. Sensors, such as door contacts, glass break sensors and infrared motion detectors, connect to an alarm that is sounded when the system is compromised. Sensors are wired to a central control panel that can deactivate an alarm by keying in the proper code. Properly installed, used, and maintained, City of Phoenix Intrusion Detection Burglar Alarm Systems are a real asset to the organization.

Every effective Intrusion Detection System is only as good as the department employees and the Central Monitoring Station that monitors it. Designated Authorized Signers must educate employees, tenants, and contract workers on the proper use of the Intrusion Detection System, how to properly enter the facility without unnecessarily setting off alarms, and how to report accidental alarm activations.

When Intrusion Detection Systems are misused and not operated properly, they can become a liability to the City. The Phoenix Police and Fire Departments as well as the Central Monitoring Station, must spend a significant amount of time and money handling

and responding to false alarm activations. As the Designated Authorized Signers and system users, you may also experience the inconvenience of false alarms at the facilities you maintain.

11.2 – Alarm Permit Subscriber Permit Application Form

An alarm subscriber permit application form is required for all Intrusion Detection Systems monitored by the City of Phoenix Central Monitoring Station. The form must be completed by the Designated Authorized Signer and forwarded to the Police Department Code Enforcement Unit when a new Intrusion Detection System is installed. The initial application fee is $17.00 and a cost center must be included on the application form before returned to the Code Enforcement Unit.

City of Phoenix facilities with an Intrusion Detection System installed that do not have a burglar alarm permit on file with the Police Department will be assessed a $96.00 fee. Designated Authorized Signers are required to complete that alarm subscriber permit form, include that department cost center, and return the application form to the Police Department Code Enforcement Unit immediately. Once the form is received and processed by the Police Department personnel a permit number is assigned to the City facility for emergency response purposes. Departments may also be subject to an assessment of $105.00 for a fire alarm activation that the Fire Department responds to if there is no permit on file.

11.3 – Annual Renewal Process

The Designated Authorized Signers and/or Responsible Party must renew the City of Phoenix Alarm Subscriber Permit and notify the Public Works Department Alarm Services staff (if the alarm system is monitored by the Central Monitoring Station) to make all necessary updates in the security system database. It is important to update the responsible party names and telephone numbers on the permit form that is returned to the Police Code Enforcement Unit as well as to ensure the Public Works Department system database reflects the changes.

11.4 – PIN Codes

Personal Identification Numbers, or PIN codes, are programmed into the Intrusion Detection System database to allow an authorized person the ability to arm and disarm a facility's burglar alarm system by use of a keypad. Any employee or contract worker requiring a PIN code is asked to select a 4-digit number that can be programmed to the system panel in the field to communicate with the keypad. PIN codes are specific to the individual and must not be shared and loaned to other individuals. PIN codes should be kept confidential and not be obvious or easy to guess. It is recommended that when selecting a PIN code that the use of bankcard PIN numbers or the last 4-digits of social security numbers are not used for security reasons. Designated Authorized Signer and/designees must notify the Public Works Department of any changes in status to ensure accurate data is maintained in the security system.

Generic PIN codes are not allowed for security and identification purposes, but may be acceptable based on certain operational needs.

11.5 – Responsible Party

The Responsible Party is the person(s) designated by the department to handle alarm activations and the person(s) responsible for responding to the facility in the event of an emergency after hour issue. When alarm activations are received in the Central Monitoring Station, police staff will notify the Responsible Party of the alarm type and condition. Police and/or Fire may request the responsible party respond to the facility. The responsible party is required to have an established PIN code, a badge and appropriate keys (where applicable) to the facility to properly investigate the alarm issue(s).

It is important for Designated Authorized Signers to identify a minimum of three (3) people who can be primary contacts and responsible parties for after-hour alarm notifications. Contact information for responsible parties must be kept up-to-date and on file with the Public Works Department, the Central Monitoring Station or their appropriate monitoring agency.

11.6 – False Alarms

False alarms are a problem for everyone: the City, Designated Authorized Signers, the Central Monitoring Station and the Police Department. With the growing number of alarm systems being installed and used throughout the City of Phoenix, all facility Responsible Parties and users must be aware of how to correctly operate their internal systems.

In addition to the personnel costs to the City of Phoenix, there are other items that affect police response to false alarms. False alarms are costly and divert Police Officer time

away from calls that may be real emergencies. Article IX of the City Code describes the duties of alarm subscribers, proprietor alarm owners, and alarm businesses and explain how false alarms are defined.

The majority of false alarms are caused by human error. False alarms caused by human error are the easiest to prevent. It is extremely important that Designated Authorized Signers, Responsible Parties, and users understand how to operate the alarm system in order to prevent unfortunate mistakes that result in a Police emergency response and unnecessary cost to the City of Phoenix.

Everybody must do their part to reduce the number of false alarms generated citywide. A few tips:

- Make sure everyone who has access to the premises knows how to operate the alarm system and knows how to clear false alarm activations from the keypad.
- Immediately call the Central Monitoring Station and inform security staff of any errors and false alarm activations.
- If there are any changes at the facility such as remodeling that may affect the security system devices, such as a motion detectors or panic buttons, notify the Public Works Department Alarm Services section.

- Make sure Responsible Party names and after-hour contact details are current and up-to-date.
- Every person using the alarm system keypad must have their own PIN for verification purposes with the Central Monitoring Station.
- During monsoon weather, the Responsible Party and/or staff should double check all doors and windows to make sure they are secure and will not blow open.
- Conduct monthly observations of alarm system devices such as motion detectors to make sure there are no obstructions, dust build up, and that building doors and windows are securing properly.
- Report problems immediately to Public Works Department Work Control by calling 602-262-6732.

11.7 – Preventative Maintenance Inspections

City of Phoenix Code requires an annual preventative maintenance inspection of all security alarm systems. Preventative Maintenance can save the City unwarranted costs, eliminate false and trouble alarms issues, and reduce expensive repairs when performed by the Public Works Department Alarm Services trained professionals.

Designated Authorized Signers should establish annual auto-generating preventative maintenance inspection work orders by contacting the Public Works Department Work Control at 602-262-6732. Public Works Department Alarm Services staff can assist departments with the above process.

Section 12: Keys

12.1 – Introduction

Physically keys cannot be turned off or deactivated electronically to prevent use. It is the responsibility of the Designated Authorized Signer to train and educate employees and contract workers on the importance of keeping track of keys that are issued by the City of Phoenix.

City employees requiring keys to perform the duties of their position must safeguard them in the same manner as they would ID/Access Badges.

There are times when a contractor and/or their workers may require a key to be issued to complete City approved work or services. A key may be issued only upon written authorization from the applicable contracting Designated Authorized Signer. **A key shall be authorized only when no other reasonable means of access is available.** All policies described for issuing badges to contractors and their workers must be followed to issue keys (see AR 4.44, Section 4.J.).

12.2   Responsibility of the Site Key Liaison
The Site Key Liaison is responsible for tracking all keys assigned to their site. These responsibilities include recording and maintaining all key information in a site database. It is suggested that the Key Liaison retain a copy of the key issue form from the key holder, in order to maintain a written record with signature and date for when that person received and returned the key.

12.3 – Key Issue Instructions
All keys are issued to Site Key Liaisons by Alarm Services. Keys will then be issued to personnel on-site and tracked by the Site Key Liaison. Alarm Services requires original key issue forms with original signatures to release keys. The following steps need to be completed for a key to be issued or re-issued:

1. Submit a request for a work order to Work Control (602-262-6732).
2. Record the work order number on the top left of the Key Request Form (See the Intranet site for the most current Key Request Form.)
3. Date the form at the top right hand side.
4. Fill in your information on the "City of Phoenix Employee" line.
5. Mark any applicable boxes in the "check all that apply" section: "New issue, Duplicate, Master," etc.
6. In the "Key Number 1" box, record the key information and include all letters and numbers on the existing key if available. For example: 22x13 NA; 10M03 NC; AD HE. Building numbers refer to facilities with multiple buildings at the site. Boxes 2 and 3 can be used for additional keys, but request only one key code per box. Record the number of key copies requested of each code in the "copy no." box.
7. Sign, and fill in all of the information on the "key holder's signature" line at the bottom of the form, middle line.
8. Read and initial the bottom two lines in the "NOTE" section.
9. Forward the form to your Designated Authorized Signer to sign, filling in all of the information on the "key authorizer's signature" line at the bottom of the form, top line.
10. The Designated Authorized Signer should then forward the form to Alarm Services at the address at the top of the form. (Calvin C. Goode Building, 251 W. Washington, 2nd floor Mezzanine.)
11. Alarm Services will e-mail or call when keys are ready. Keys can be picked up at the Calvin Goode Building 2nd floor.

12.4 – Key Return Instructions

The following instructions shall guide the return of a key when it is no longer necessary for any reason.

1. Make any necessary changes in the site database.
2. Fill out a key issue/return form. (See Intranet site for the updated form.)
3. Mark the form "Return" in the "check all that apply" section.
4. Fill in all of the information in the "Received key(s) from" section.
5. Record the key information, for example: 22x13 NA, 10M03 NC, AD HE and building information in key box #1, 2 or 3 that are to be returned.
6. Sign, and fill in all of the information on the "key holder's signature" line at the bottom of the form, middle line.
7. Return the form and keys to Alarm Services at the address on the top of the form. (Calvin C. Goode Building, 251 W. Washington, 2nd floor Mezzanine.)

8. Alarm Services representative will sign the "key received by" section and return the form to you as a receipt.

12.5 – Key Duplication

All keys are property of the City of Phoenix. Duplication of keys by anyone other than authorized personnel is prohibited.

12.6 – Terminated or No Longer Required

Keys must be obtained from employees and contract workers and returned to the Designated Authorized Signer before the end of their last working day with the City of Phoenix and/or with the contracting department.

12.7 – Lost/Stolen Keys

Lost and stolen keys shall be immediately reported to the Designated Authorized Signer. Employees are required to file a Police report and obtain a Department Report (DR) number for lost and stolen keys. If a new key is required, the Designated Authorized Signer must generate a work order by contacting Public Works Department Work Control and complete and sign a new Key Request Form for the employee. Depending on the type of key and what facilities are controlled by the key, departments may be required to re-key the facility and absorb all costs associated to the re-key.

For contractors, lost and stolen keys shall be immediately reported to the contract worker's contract manager. Contract workers are required to file a Police report and obtain a Departmental Report (DR) number for lost and stolen keys. The contracting department must establish a method for reporting lost and stolen keys during after-hours. The Contractor and contracting department may be required to bear the cost for re-keying locks and replacing keys. If another key is required, a new key request form must be completed and signed by the contracting department's Designated Authorized Signer.

Section 13: Auditing

13.1 – Introduction

Frequent audits will depend on the level of security needed in each facility/area. Audits can be conducted in various forms. In high risks area, the department may want every employee to show their badges and keys to assure they are still active and in the employee's possession. In lower risk areas, the audit can be performed by coordinating with the appropriate Human Resource liaison and working closely with the appropriate Badge Office. Any questionable issues related to auditing badges, access, any keys should be researched and the appropriate action taken to ensure assigned badges and keys are with the correct personnel and access is restricted to only those areas that are approved.

Keys should periodically be visually reviewed to ensure that employees are still in possession of the keys assigned to them.

Departments are responsible for developing an audit plan for reviewing access for their areas at least once annually (for high-risk areas, it is recommended that audits be performed more frequently). The audits should include, but not limited to:

A.R. 4.45
- Contract Worker Disclosure Forms copies for each contract worker
- Review of contract company files
- Name of firm and/or internal staff that conducted the background checks
  - Type(s) of Background Checks conducted
  - Background Check results
- Confirmation that the contract worker is still employed with the company
- Confirmation that the contract worker has an active badge in their possession

A.R. 4.44
- Employee's badge (physical inspection)
- Badge access (electronic access)
- Keys (physical inspection)
- Employee's with PIN Code access (electronic access via burglar alarm system key pads)
- Responsible Party (RP) Data and after-hour contact numbers
- Facility Dispatch Instructions

Badging Offices and the City Auditor may also perform audits as they deem necessary.

12.2 – Violations
Violations of the Badge and Access Controls and Contract Worker Background Check Administrative Regulations may result in disciplinary action.