

Steps for Obtaining Badge Access to South Mountain Towers

1. The contractor or contractor's organization will contact the City of Phoenix Parks and Recreation Department at (602) 261-8605 or southmountaincontracts@phoenix.gov to request access. A packet will be emailed to the requestor.
2. Contractor receiving the badge will complete the forms listed and contained in this packet and present in person to the **Parks and Recreation Department, 200 West Washington Street, 16th Floor, Phoenix, AZ 85003**:
 - Badge Responsibility Agreement Form
 - Contract Worker Clearance Information Form
 - City contract # and contract end date must be on form
 - Background Check Form
3. Contractor will go to the Payment Service Center with \$55.00 (cash, check or credit) located at the address below to pay for their badge.

**The City of Phoenix
Payment Service Center
305 West Washington Street
1st Floor**

4. Contractor will go to the badging office located in the lobby of the Calvin Goode Building and show badging staff the paid receipt and photo identification for the issuance of the badge.

**Calvin Goode Building
251 West Washington Street
1st Floor**

City of Phoenix
Parks and Recreation Department
Badge Responsibility Agreement Form
South Mountain Towers

1. Contract Worker shall be obligated to all terms and conditions of the contract. Contractual agreements shall be binding upon involved parties and their successors and assignees.
2. Badges shall be displayed on the person and be visible at all times while on City business.
3. Contract Worker must not loan, borrow or share badges.
4. The person to whom a badge has been issued shall be held responsible for its use until it has been properly returned to the department's badge liaison, or the appropriate badging and/or security office.
5. Contract Worker found to be in possession of an unauthorized badge shall be liable for its use and may be subject to disciplinary or legal action.
6. Contract Worker is responsible for immediately notifying the City of lost/stolen badges so that cards can be deactivated and the appropriate precautions taken. If they are unaware of whom to notify, they shall contact their supervisor to find the appropriate contact. Contractors shall call 602-261-8605 and leave a voice mail to report lost/stolen badges during after-hours.
7. Contract Worker shall provide a police report for any stolen badges.
8. The Badging Office will charge Contract Worker a fee to reissue badges unless a police report is provided. Recovery cost may be waived with police report submittals.
9. Contract Workers shall not tamper, interfere, compromise, modify or circumvent any security system, measures or procedures.
10. Contract Worker shall not allow non-badged persons to follow them into a restricted or controlled environment unless being escorted by a badged City employee.
11. Contract Worker must take precaution to secure their badge. Badges should never be left on a desk, in a vehicle or any place exposed to the public or unauthorized users.
12. Badges must be returned to the appropriate badging and/or security office when no longer needed or upon the Contract Worker termination / transfer. Failure to return badges may result in recovery cost.
13. Contract Worker shall in no way modify or duplicate their badge. Physical alteration and/or modification of a badge without permission from the Parks and Recreation Department may result in the Contract Worker having to be issued a new badge at the Contract Worker's expense.

Print Name: _____

Signature: _____

Phone Number: _____

License Contract Number: _____

CONTRACT WORKER CLEARANCE INFORMATION FORM South Mountain Towers

(COMPLETE TOP SECTION AND SUBMIT ORIGINAL WITH LEGIBLE COPY OF OFFICIAL PHOTO ID)

DATE: ____ / ____ / ____ CONTRACT NUMBER: _____

CONTRACT COMPANY NAME: _____ CONTRACT END DATE _____

Last Name: _____ First: _____

Middle Name: _____ Date of Birth: ____ / ____ / ____

Other Names Used: _____

Place of Birth: _____ Sex: _____ Race: _____

Address: _____ City: _____

Zip Code: _____ Business email address _____

List All Cities/States Lived in the Last 7 Years (attach additional sheet if necessary):

Height: ____' / ____" Weight: _____ Hair Color: _____ Eye Color: _____

Social Security Number: _____ - _____ - _____ INS Number: _____

HAVE YOU BEEN CONVICTED OF A MISDEMEANOR, A FELONY, PLACED ON PROBATION, CONVICTED BY MILITARY TRIAL, OR GIVEN A SUSPENDED SENTENCE IN COURT? YES _____ NO _____

DO YOU HAVE ANY CRIMINAL CHARGES FOR WHICH YOU ARE AWAITING TRIAL? YES _____ NO _____

DO YOU HAVE ANY CURRENT AND/OR OUTSTANDING WARRANTS PENDING? YES _____ NO _____

IF YES, PLEASE EXPLAIN:

Responding "Yes" to the above questions does not automatically disqualify you from access to a City facility. However, failure to accurately respond will result in disqualification or discharge from access.

I understand that if I am convicted of a misdemeanor, a felony, placed on probation, convicted by military trial, given a suspended sentence in court, or have any criminal charges for which I am awaiting trial after I receive a City of Phoenix ID/Access Badge, that **! must report this to the City of Phoenix and my employer. The City will then determine if I must surrender my ID/Access badge and/or key(s).**

The information I have provided on this Contract Workers Clearance Information form is true, complete and correct to the best of my knowledge and belief, and is in good faith. I understand that a knowing and willful false statement on this form can be grounds for disqualifying me access and may be punishable by law.

Authority: The authority for collecting this information "City of Phoenix", and 49 U.S.C. 44936, "Employment Investigations and Restrictions".

Purpose: This information is needed to validate your identity and to retrieve your criminal history record to evaluate your suitability for access to City of Phoenix owned/operated facilities and for a City of Phoenix ID/Access badges and/or key(s). Your Social Security Number (SSN) will be used as your identification number in this process and to validate your identity. Furnishing this information, including your SSN, is voluntary; however failure to provide it will prevent the completion of your criminal history records check, without which you may not be granted electronic access.

I hereby give _____ N/A _____ permission to conduct a background check consistent with City of
(Contract Worker's Printed Name)

Phoenix, Police Department's Employment Services requirements. I also understand in some circumstances, background check information may be shared with City of Phoenix personnel.

Contract Worker's Printed Name: _____ **Date:** _____

Contract Worker's Signature: _____

Contract Worker's Phone Number: (_____) _____ - _____

Contract Worker's Email: _____

To: City of Phoenix, Parks & Recreation Department

Jona Banks, Administrative Aide

From: Company Name _____

Contact Person _____

Subject: Maximum Level Background Check

I have reviewed the following type(s) of maximum level background check(s) provided by

_____ for _____ employed by _____

(background company name)

(employee name)

(name of company)

Pass N/A

___ ___ Conducted screening required by Arizona Revised Statute (A.R.S) 41-4401 to Check for the Legal Arizona Worker Status through use of E-Verify or other means of checking for Legal Worker Status.

___ ___ Real Identity Check / Legal Name

___ ___ Criminal History Search – Felony & Misdemeanor Records Checks for any county in the United States, State of Arizona, plus any other Jurisdiction where the Worker has lived at any time in The preceding seven (7) years.

___ ___ Sex Offender Search

___ ___ Credit Report Search

___ ___ Motor Vehicle Report Search

___ ___ Other _____

Based on the information contained in the above report(s) I ACCEPT / DENY _____ to have access to South Mountain Tower Sites.

(circle one)

(worker's name)

_____ Date _____ Telephone number _____

(signature)



City of Phoenix

ADMINISTRATIVE REGULATION	A.R. NUMBER
	4.44 Revised
SUBJECT	FUNCTION
	Legal Matters Page 1 of 11
	EFFECTIVE DATE
CONTRACT WORKER IDENTIFICATION AND ACCESS CONTROLS	September 1, 2018
	REVIEWED DATE

This Administrative Regulation (AR) addresses Contractors identification and access to City of Phoenix facilities, which is essential to the smooth operation of the City. There is also the equally critical concern for the security and integrity of facilities, their contents, and the safety of employees and contractors. Integral to both concerns is a well-defined and workable identification and access control policy.

Any variance from this AR (unless due to federal/state regulations) must be reviewed and approved by the Security and Access Review Committee and the Office of Homeland Security and Emergency Management.

The Security and Access Review Committee is made up of representatives from City departments and is charged with assuring that access is consistent and controlled. The committee is co-chaired by the Public Works Department and Office of Homeland Security and Emergency Management.

Contractors are required to comply with the security measures at each individual work location within the City.

Questions regarding this AR should be directed to the Public Works Department Badge Imaging Office at 602-534-4611.

I. PURPOSE

The purpose of this AR is to provide guidelines for managing Contract Workers access to City facilities and City assets, to enhance the personal safety of employees, contractors, the public, and to limit the City's exposure to loss.

This regulation governs Contract Workers 1) badge access cards, 2) identification cards, 3) keys, 4) alarm PIN (personal identification number) codes, or 5) any other means of access that may be implemented that give access to City facilities and offices. The City department must ensure the appropriate forms and language is included in the contracts per the level of access and scope of work.

II. DEFINITIONS

Contract Worker means a person performing services for the City such as:

- an individual who has a contract with the City;
- a worker of an entity that has a contract with the City;
- a worker of a subcontractor of an entity that has a contract with the City; or
- a worker of a tenant/lessee of the City.

Contractor or Consultant means a person or entity that has a contract with the City to perform services for the City.

Criminal Justice Information Services (CJIS) outlines the security precautions that must be taken to protect sensitive information like fingerprints and criminal backgrounds gathered by local, state, and federal criminal justice and law enforcement agencies. Contact the department's badging office or badging liaison for facilities that are identified as Criminal Justice Information System (CJIS) sites.

III. RISK ASSESSMENT AND LEVELS OF ACCESS

- A. The City is made up of numerous departments that provide a wide range of services. As such, the City faces exposure to a wide variety of risks. As a result, each Department will perform its own independent risk analysis to determine desired level(s) of access for contractors.

To assist in this analysis, access can be categorized according to three different general levels, as defined below. These levels of access and their definitions and descriptions are not all inclusive, but may be used by departments as a guide to aid them in assessing their areas. Areas may be a combination of these types.

1. Public access – areas where the public has access to conduct business with city operations during established business hours.
2. Limited/Controlled Access – areas where the public may be permitted access to general areas but there is a need to limit or supervise their access due to risk of loss (of assets, cash or information).
3. Restricted Access – areas where there is no need for access to anyone other than those with a specific need to work in the area or places in which losses in the area would be substantial and disruptive to the ongoing business of the organization.

- B. A risk analysis should consider the following factors:

- The probability of loss occurring;
- The impact the loss may have on operations or the organization;
- The feasibility and cost/benefit of implementing security measures;
- The personal safety of employees and the public.

- C. A guide for determining levels and security needs has been included at the end of this AR (Levels of Access Guide).
- D. Based on the access levels(s) determined from the analysis, the Department Director or designee can determine the following:
- What type of access controls are justified - open to public, key locks, card readers, alarms, personal identification numbers (PIN), security guard, etc.;
 - How Contract Workers will be identified – require Contract Workers to wear their badge, and/or use badge to obtain access through use of card reader;
 - What level of approval authority is required to make access permission decisions - Department Director, Deputy level, or supervisory level.
- E. For further guidance in assessing risks and level of security, the department may contact the City of Phoenix Police Department – Threat Mitigation Unit.
- F. Regardless of the levels of access established, departments should be prepared to implement more stringent access controls in the event of a change in the National or Local threat level.

IV. AUTHORIZATION FOR ACCESS

- A. The Department Director or designee will determine the appropriate method(s) to manage Contract Worker access to areas under their jurisdiction. Methods of access control may include, but are not limited to, visual inspection of identification to permit entry, badge reader devices that release locks on keyed doors, alarm PIN codes, and/or any other means of access controls that may be implemented.
- B. The authority of the Department Director or designee to approve access is limited to those areas under the Department Director's authority. The Chief Presiding Judge, or designee, will have authority to approve access to areas in the Phoenix Municipal Court facility.
- C. Each department will establish and maintain an Access Authorized Signer List. The list will 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 can 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.
- D. Authorization to grant contractor access will be documented by the requesting department prior to the issuance of the badge, key, PIN code, etc. Documentation will include the following:
- Location and times of access needed;
 - Approval signature of Contract Workers;
 - Approval signature from the department's authorized signer (per established list discussed above), from every department/function whose areas will be accessed.

- E. Some Public Works, Information Technology Services and other critical response personnel provide services to departments around the clock and must be able to access areas often with little notice (for example, electricians and computer technicians). Departments must work with these internal service providers to develop a method of communicating and coordinating access for these contractors OR guaranteeing an escort be made available at all times.
- F. Departments who are not responsible for assigning their own access must be notified by the responsible assigning party whenever a new contractor is assigned access to their facility. Departments are responsible for requesting access permission for their contractors in building areas that they do not manage.

V. BADGES / IDENTIFICATION CARDS

- A. Departments will ensure that all Contract Workers have an approved City issued picture identification badge /card, which is visible at all times.
- B. Police and Fire Departments will issue department specific identification cards that will be carried by Contract Worker while on duty. Aviation Department Contract Workers will have badges that comply with federal regulations.
- C. For all other departments, badge templates must contain the following:
 - 1) Front of badges will contain:
 - Contract Worker's picture
 - Contract Worker first and last name
 - City Bird emblem
 - Contract Worker's Company name
 - Expiration date
 - Badge expiration dates will be the contract term or 5 years whichever is shorter. Expiration dates will be input into the badging system so that cards will be deactivated upon expiration.
 - 2) Back of badge will contain:
 - Information on how to return the badge if found
 - Statement indicating that the badge is property of the City and must be surrendered upon request of the issuing department
 - 3) Badges will be identified by different border colors based on the level of background check completed.
 - Standard = Yellow
 - Maximum = Green
 - Maximum = Green with Red CJIS lettering

Contract Worker maximum or maximum CJIS background checks will be valid for the contract's term or three years whichever is shorter, unless related to healthcare or nursing home facilities.

D. Temporary badges

A temporary badge is defined as a non-picture badge that will only be used by visitors, volunteers, interns, tenants, and employees who forget their badge, etc.

Departments will be assigned temporary badges upon request. Departments with temporary badges will be responsible for designating a badge custodian and establishing procedures to safeguard and control the inventory of badges.

Departments should use and maintain as few temporary badges as needed to support operations. Active temporary badges should be limited since it allows the holder the ability to access areas unescorted.

Temporary badges can be "Active" or "Inactive".

- 1) Active temporary badges will allow the holder to access areas through the use of a card reader. The badge will have a deactivation date set in the badging system for a maximum of five days. After five days, the Department Approver can extend the temporary non-picture badge for an additional five days. A background check must be performed prior to issuing anyone an active badge.
- 2) Inactive temporary badges act as a "visitor's pass" and will give the holder access to non-public or public areas. It can NOT be used in a card reader; thus, the person must be escorted into any restricted areas. A badged City employee must be responsible for ensuring the escorted person is within their span of control at all times (at a distance where they can visually see the person).

E. Licensees to Operate and Maintain Electronic Communications

The City has license agreements with different users at various sites. The sites are used by the licensees to operate and maintain equipment and facilities for electronic broadcasting communications. Since these users have different requirements any deviations must be reviewed and approved by the Security and Access Review Committee. For instance, security and badging policies and procedures for South Mountain Communication Tower site will be developed by Parks and Recreation Department and the Public Works Department, with approval from the City of Phoenix Police Department.

VI. BADGE HOLDER RESPONSIBILITIES

Contract Worker responsibilities include, but are not limited to:

- a) Contract Worker shall be obligatory to all terms and conditions of the contract. Contractual agreements shall be binding upon involved parties and their successors and assignees.
- b) Badges shall be displayed on the person and be visible at all times while on City business at City facilities.
- c) Contract Worker must not loan, borrow or share badges, keys or PIN codes.
- d) The person to whom a badge has been issued shall be held responsible for its use until it has been properly returned to the department's badge liaison, or the appropriate badging and/or security office.
- e) Contract Worker shall read and sign a Contractor Badge Key Intrusion Responsibility Agreement acknowledging their responsibilities related to safeguarding and caring for their city issued badge.

- f) Contract Worker found to be in possession of an unauthorized badge shall be liable for its use and may be subject to disciplinary or legal action.
- g) Contract Worker are responsible for immediately notifying the City of lost/stolen badges so that cards can be deactivated and the appropriate precautions taken. If they are unaware of whom to notify, they shall contact their supervisor to find the appropriate contact. Contractors must work with the contracting department to establish a method for reporting lost/stolen badges during after-hours.
- h) Contract Worker shall provide a police report for any stolen badges.
- i) The badging function will charge Contract Worker a fee to reissue badges unless a police report is provided. Recovery cost may be waived with police report submittals.
- j) If a badge is found, Contract Worker must notify the department's badge liaison, or the appropriate badging and/or security office.
- k) Contract Worker shall use their assigned access cards to gain entry into work areas that have card readers. Keys should only be used in an emergency situation as it will cause alarms to be activated.
- l) Contract Workers shall not tamper, interfere, compromise, modify or circumvent any security system, measures or procedures.
- m) Contract Worker shall not allow non-badged persons to follow them into a restricted or controlled environment unless being escorted by a badged City employee.
- n) Contract Worker shall ensure doors are secure and never left open.
- o) Contract Worker must take precaution to secure their badge. Badges should never be left on a desk, in a vehicle or any place exposed to the general public.
- p) Badges must be returned to the appropriate badging and/or security office when no longer needed or upon the Contract Worker termination / transfer. Failure to return badges may result in recovery cost.
- q) Contract Worker shall question the presence of un-badged persons and report infractions.
- r) Contract Worker shall not duplicate badges.
- s) Contract Worker shall in no way modify their badge in any way other than designated by their department security liaison. Physical alteration and/or modification of a badge without permission from the department security liaison, may result in the contract worker having to be issued a new badge at the contract workers financial expense.
- t) Contract Workers will not vehicle tailgate (follow another vehicle without badging in) at any entrance gate or exit.

Contracting Department responsibilities include, but are not limited to:

- a) Contracting departments will ensure that appropriate background checks are completed as a condition of employment (refer to AR 4.45). Badges will only be issued to contractors who have successfully passed a background check. Contract Worker maximum or Criminal Justice Information System (CJIS) background check will be valid for the contract term or three (3) years whichever is shorter.
- b) Contracting departments will ensure that contractors read and sign a Contract Worker Badge/Key/Intrusion Detection Responsibilities Agreement acknowledging their responsibilities related to safeguarding and caring for their city issued badge. The information found in an Agreement may vary between departments and/or locations based on the level of security maintained in each area, but should include the badge holder responsibilities outlined in section VI of this AR. Departments are responsible for maintaining Contract Worker Badge/Key/Intrusion Detection Responsibilities Agreement for each contractor.
- c) Contracting departments must ensure that badge applications includes the contract number and badge expiration date.

- d) Contracting departments must establish an authorized signer or badge liaison list for their department to sign off on contract workers badge applications.
- e) Department Badge Liaisons are responsible for notifying the appropriate badging and/or security office of needed access changes within 24 hours so that changes can be made in a timely manner. Badge Liaisons must also be available to address any access related issues that may arise.
- f) In some cases, the contractor's information (i.e., Person of Interest (POI)) must be entered in eCHRIS prior to issuance of a badge. This ensures consistency between badging and human resource systems. Contracting departments are responsible for initiating and facilitating the process.
- g) Contracting departments will ensure that contractors provide the appropriate badging and/or security office with a valid government issued picture identification in order to obtain a City issued badge.
- h) Contracting departments must notify the appropriate badging office to deactivate contractors' badge access as soon as possible but no later than 24 hours after termination. Departments are responsible for collecting badges from terminated contractors before the end of their last day of employment. (The contract must document that the contractor will bear the cost of badges and background checks).
- i) Contracting departments must establish a method for reporting lost/stolen badges during after-hours. This method should be outlined on the Contractor Badge Responsibility Agreement.
- j) Contracting departments will require a police report be filed for any stolen badges. A new badge application must be filled out before a replacement badge can be issued at no charge.
- k) Contracting departments will require a cost recovery fee for all lost or damaged badges.
- l) Contracting departments will ensure that if a badge is physically altered, the department will initiate the procedure for a new badge for that Contract Worker at the Contract Worker's financial expense.

VII. KEY HOLDER RESPONSIBILITIES

Contractors may be issued a key only upon written authorization from the applicable Contracting department or Key Control Custodian. A key will be authorized only when no other reasonable means of access is available.

Contract Worker responsibilities include but are not limited to:

- a) Any obsolete or unneeded keys should be returned to the contracting department or Key Control Custodian.
- b) Master Keys
 - 1) Master or sub master keys - keys that fit more than one keyway or override operating keys or keys at any high security areas require contracting department authorization.
 - 2) Duplication - All keys are property of the City. Duplication of keys by anyone other than authorized personnel is prohibited. No Department will authorize duplicate keys from another department without appropriate approval from that department.
 - 3) Keyways - No one is allowed to purchase keyways used by another department. Key supply contractors must be given a list of authorized signers and only issue stock with the approval of these individuals. This requirement will be documented in the contract between the City and the supplier.

- c) Terminated Contract Employees – Keys must be obtained from contractor(s) before the end of their last day of employment or contract termination. Failure to return keys may result in replacement cost.
- d) Contract Worker to whom a key has been issued will be held responsible for its use until it has been properly returned to the department's Key Control Custodian.
- e) Contract Worker found to be in possession of an unauthorized keys shall be liable for its use and may be subject to disciplinary or legal action.
- f) Contract Worker must take precaution to secure their keys. Keys should never be left on a desk, in a vehicle or any place exposed to the general public.

Lost/stolen keys

- a) Lost/stolen keys will be immediately reported to the Contract Worker supervisor, department Key Control Custodian and applicable Locksmith Services.
- b) City will advise Contract Worker that a police report must be filed for any stolen keys.
- c) Contract departments may be required to bear the cost of re-keying locks and replacing keys if the contract fails to place this responsibility on the contractor or the contractor fails to pay the charges due to a City error or negligence. The Department may choose to subrogate those costs from the Contractor.
- d) Another key request form must be completed and signed by the approving authority.

Contracting department responsibilities include, but are not limited to:

- a) Contracting department will appoint a Key Control Custodian(s) to coordinate key control and to assure that keys are adequately maintained within the department.
- b) Contracting department must establish a method for reporting lost/stolen keys during after-hours.
- c) Contracting department will establish a policy regarding acceptable loss of keys. It is recommended that affected door locks be changed and new keys issued when more than 5% of keys for any given series cannot be accounted for. It is mandatory that locks be changed when more than 20% of keys cannot be accounted for.

VIII. INTRUSION DETECTION SYSTEM RESPONSIBILITY

Many areas around the City are equipped with Intrusion Detection Systems (alarms) and other special systems. Contract Workers must be made aware of these systems and instructed on how to properly enter the area without unnecessarily setting off alarms (for example, never use a key to open a door equipped with a card reader unless it is an emergency situation).

- A. PIN Codes – Personal Identification Number (PIN) Codes are programmed into an intrusion detection system to allow authorized Contract Workers the ability to arm and disarm the facility's intrusion detection alarm system by use of a keypad. PIN codes are to be specifically used by the individual to whom it is assigned. Generic PIN codes will not be allowed. It is recommended that contractor not use their bank card PIN number or the last 4-digits of their social security number. Issuing department must be notified of any change in contractor status to ensure accurate data is maintained in the security system. Alarm PIN codes must be memorized or secured in the same way as badges and keys.
- B. False Alarms - It is imperative that Contract Workers immediately notify the Central Monitoring Station or their appropriate monitoring agency of all false alarm activations.

False alarms are costly and divert police officer time away from calls which may be real emergencies. Article IX of the City Code describes the duties of alarm subscribers, proprietor alarm owners and alarm businesses, and explains how false alarms are defined.

Contracting department will ensure:

- a) Contract Worker is aware of Intrusion Detection Systems (IDS) and how to properly enter the area without unnecessarily setting off alarms (i.e.), never use a key to open a door equipped with a card reader unless it is an emergency).
- b) Contract Worker shall only use PIN codes that are specifically assigned to the individual.
- c) Contract Worker keeps PIN codes confidential, not be obvious or easy to guess, and not share or loaned to others.
- d) Contract workers immediately notify the Central Monitoring Station or their appropriate monitoring agency of all false alarm activations and the contracting department. False alarms are costly and divert police officer time away from calls which may be real emergencies.

Contracting department responsibilities include, but are not limited to:

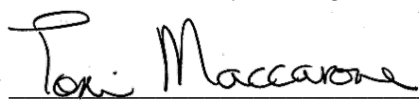
- a) Contracting department will ensure everyone who has access to the premises knows how to operate the Intrusion Detection Systems and knows how to clear false alarm activations from the keypad.
- b) Contracting department will ensure that everyone using the alarm system keypad to have their own PIN for verification purposes with the Central Monitoring Station.
- c) Contracting department will immediately report problems to Public Works Department Facilities Support Services at 602-262-6732 when issues arise as to avoid false alarms.
- d) Contracting department will notify PIN users of any impending changes at the facility such as remodeling that may affect security system devices.

Violations of this AR may result in disciplinary action up to and including termination.

VIII. QUESTIONS

Questions regarding this AR should be directed to the Public Works Department Badge Imaging Office at 602-534-4611.

ED ZUERCHER, City Manager

By 
Toni Maccarone,
Acting Deputy City Manager

LEVELS OF ACCESS GUIDE

This table can be used as a guide in determining what type / level of access is needed in an area.

Exposure Type	Potential Target	Risk	Security Risk Level	Typical Features	Security Requirements
Theft of tools, equipment, computers, Petty cash, & other low value assets (<\$5,000).	Shops Warehouses Storerooms Cash drawers General office areas	(1) Small monetary loss (2) Loss of low value assets	Standard Risk Level	Partially secure - area is not secure but identification system makes detection likely. Badging & Key Control Systems Effective Administrative Controls. *	(1) Identity of person entering area should be known and verifiable. (2) Person entering must have a demonstrated and approved need for access. (3) Public must be escorted by a badged City employee.
Violence, Irrational Behavior	Employees of the City Elected officials	(1) Injury or death (2) Loss of employee confidence	Standard Risk Level or Maximum as applicable**	Partially secure - area is not secure but identification system makes detection likely. Badging & Key Control Systems Effective Administrative Controls. *	(1) Identity of person entering area should be known and verifiable. (2) Person entering must have a demonstrated and approved need for access. (3) Public must be escorted by a badged City employee.
High Value Theft (> \$5,000)	Servers, Databases, Money Rooms Equipment	(1) Large monetary loss (2) Loss of valuable assets (3) Public criticism	Maximum Risk Level	Very secure – physical barriers surround areas that are very difficult to breach. Any breach would be detected. Badging & Key Control Systems Effective Administrative Controls. * Card Readers at all entry points.	(1) Identity of person entering area should be known, verifiable and documented. (2) Person entering must have a demonstrated and approved need for access. (3) Public must be by escorted a badged City employee.

<p>Data Theft Infrastructure Attack</p>	<p>Data processing centers Billing Centers Water plants Communications centers Infrastructure Elections Areas HIPAA or State or federally mandated to protect HAZMAT areas</p>	<p>(1) Substantial business interruption (2) Substantial damage (3) Substantial monetary loss (4) Public criticism and lack of confidence (5) Fines and liability (6) Terrorism (7) Catastrophic Loss (8) Injury and death (9) Loss of public's sense of security</p>	<p>Maximum Risk Level</p>	<p>Completely Secure – formidable physical barriers surround areas that are virtually impossible to breach. Any breach would be detected. Badging & Key Control Systems Effective Administrative Controls* Card readers at all entry points Record of persons entering- identity, date and time Video surveillance at entry points</p>	<p>(1) Identity of person entering area should be known, verifiable and documented (2) Persons entering have had a background check with a high level of scrutiny. (3) Approval of access must be by a functional head of the facility or restricted area. This authority cannot be delegated. (4) All breaches should be detected and investigated (5) Access lists must be established and audited frequently (such as monthly or quarterly).</p>
<p>Children and Vulnerable Adults</p>	<p>Children, <i>Vulnerable Adult</i> means an individual who is eighteen years of age or older who is unable to protect himself from abuse, neglect or exploitation by others because of a mental or physical impairment Children and Elderly programs, and other Specialty programs where direct contact with these populations occur</p>	<p>(1) Public criticism and lack of confidence (2) Injury and death (3) Loss of public's sense of security</p>	<p>Maximum Risk Level</p>	<p>Very secure – physical barriers surround areas that are very difficult to breach. Any breach would be detected. Specialized Systems, Badging & Key Control Systems Effective Administrative Controls</p>	<p>(1) Per City Code 2-27; City Ordinance (formerly PCC 2-45.6 - Ord. No. G-5047, 1, Adopted 12-19-2007, eff. 1-18-2008) (2) Per ARS Section 46-141</p>

*Effective Administrative Controls include – designated administrator, clear policies & procedures stating importance of system, employees required to challenge unbadged persons & report infractions, tailgating prohibited (letting others into an area without requiring them to use their access badge), periodic audits & inspections, reliable inventory system for badges & keys, and appropriate penalties for violations of policy, and ongoing maintenance of systems, policies, etc.

** Person interacting with Elected Officials or directly working in elected official areas.



City of Phoenix

ADMINISTRATIVE REGULATION	A.R. NUMBER
	4.45 Revised
SUBJECT	FUNCTION
	Legal Matters Page 1 of 9
	EFFECTIVE DATE
CONTRACT WORKER BACKGROUND CHECKS	September 1, 2018
	REVIEWED DATE

This Administrative Regulation (AR) describes the requirement that background checks be conducted on contract workers performing work for, or on behalf of, the City. This AR applies to all new contracts and contract amendments executed on or after September 1, 2018.

The Security and Access Review Committee is made up of representatives from City departments and is charged with assuring that access is appropriate, consistent, and controlled. The committee is co-chaired by the Public Works and Office of Homeland Security and Emergency Management.

Contractors are required to comply with the security measures at each individual work location within the City.

Questions regarding this AR should be directed to the Public Works Department Badge Imaging Office at 602-534-4611.

I. PURPOSE

This AR describes the City's policy and practice for conducting background checks on contract workers. The goal of this policy is to ensure that individuals who are hired to perform work for the City do not represent a risk to the City or community due to factors in their background that are known or should have been known.

Two levels of risk have been established that require background checks to cover City contracts. The first level (Standard) involves circumstances where background checks are required and conducted by the contractor. The second level (Maximum with Criminal Justice Information Services (CJIS) as a subset of Maximum) is a background check that is conducted by the contractor, but reviewed and approved by the contracting City department, except for CJIS related and those required for children and vulnerable adults.

Criminal Justice Information Services (CJIS) background checks will be conducted by the Phoenix Police Department or the Arizona Department of Public Safety.

II. DEFINITIONS

Background check is the fact gathering process, as described in this AR, that is conducted to obtain information regarding a person's legal Arizona worker eligibility, criminal history, driving history, certifications, or other matters that might affect the person's ability or fitness to perform services for the City.

Child care provider means a center-based child care provider, a family child care provider, or another provider of child care services for compensation and on a regular basis that:

- (a) Is not an individual who is related to all children for whom child care services are provided; and
- (b) Is licensed, regulated, or registered under State law or eligible to receive federal assistance.

Child care staff member means an individual (other than an individual who is related to all children for whom child care services are provided):

- (a) Who is employed by a child care provider for compensation, including contract employees or self-employed individuals;
- (b) Whose activities involve the care or supervision of children for a child care provider or unsupervised access to children who are cared for or supervised by a child care provider; or
- (c) Any individual residing in a family child care home age 18 and older.

Contract worker means a person performing services for the City such as:

- an individual who has a contract with the City;
- a worker of an entity that has a contract with the City;
- a worker of a subcontractor of an entity that has a contract with the City; or
- a worker of a tenant/lessee of the City.

Contractor or Consultant means a person or entity that has a contract with the City to perform services for the City.

Contract Worker Disclosure ("*Disclosure*") means the contractor will require each worker who is performing work for the City under the terms of the contract to complete an affidavit of prior criminal record. The Disclosure will require the contract worker to 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 Disclosure also grants the City the right to review the background check results.

Personal Identifying Information means any written document or electronic data that does or purports to provide information concerning a name, signature, electronic identifier or screen name, electronic mail signature, address or account, biometric identifier, driver or professional license number, access device, residence or mailing address, telephone number, employer, student or military identification number, social security number, tax identification number, employment information, citizenship status or alien identification number, personal identification number, photograph, birth date, savings, checking or other financial account number, credit card, charge card or debit card number, mother's maiden name, fingerprint or retinal image, the image of an iris or deoxyribonucleic acid or genetic information.

Vulnerable Adult means an individual who is 18 years of age or older who is unable to protect himself from abuse, neglect or exploitation by others because of a mental or physical impairment. (See Arizona Revised Statutes (ARS) Section 13-3623.F.6).

Criminal Justice Information Services (CJIS) outlines the security precautions that must be taken to protect sensitive information like fingerprints and criminal backgrounds gathered by local, state, and federal criminal justice and law enforcement agencies. Contact the department's badging office or badging liaison for facilities that are identified as Criminal Justice Information System (CJIS) sites.

III. BACKGROUND CHECK

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

4. Maximum Risk Background Check for Child Care Staff Member Must Include:
 - 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. Criminal Justice Information System (CJIS) Background:
 - 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. Additional Required Background Check Based on Work Scope:
 - 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. Legal Requirements: 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

For more information regarding background check access and risk levels, see the attached Levels of Access Guide.

IV. EVALUATING RESULTS

A. Contract

The contracting department is responsible for incorporating the appropriate language, based upon the level of background check required, into the solicitation and final contract documents.

1. Standard Risk Background Checks: The contractor will be responsible for determining whether contract worker(s) are disqualified from performing work for the City under the terms of the contract for standard risk level background checks. Sole proprietors must submit a copy of their own background checks.

2. Maximum Risk Background Checks: The contracting department will review and approve maximum risk background check results provided by the contractor. Information to verify the results will be returned to the contractor after the City's completed review. The City may set up a secure folder or drop box for confidential materials.
 - The City will not keep records related to background checks once they are confirmed.
 - The City will only respond with an "approve" or "deny."
3. Criminal Justice Information System (CJIS) Background Checks: The Police Department Local Agency Security Officer (LASO) must review and approve all CJIS background checks.

B. Requirements

1. The Department will obtain a list of eligible contract workers from the contractor. This process must be completed prior to the contractors starting work.
2. The contract worker is to work directly with the contractor, not the City, to resolve any disputes related to the background check process or any outstanding criminal history records check information.
3. 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:
 - a. 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 worker is disqualified.
 - b. Not all criminal convictions or other negative information obtained in the background check will disqualify the contract worker from providing services or working under the contract. The contracting department (for maximum risk levels) must evaluate the relevance of the information received to the services that will be provided.
 - c. To determine if a contract worker's negative background information disqualifies that person, these factors should be analyzed:
 - Duties of the specific position.
 - Time, nature, and number of negative events / convictions.
 - Attempts and extent of rehabilitation efforts
 - The relation between the duties of the job, and the nature of the crime committed.
 - d. The analysis of whether any item in a background check is a potentially disqualifying factor involves looking at the contract work requirements, scope of work, where the work is to be done, the access to restricted 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 the contract requirements. An example of this analysis would be as follows:
 - Standard Risk Background Check: For a contract worker requiring a standard risk background check, potentially disqualifying convictions could 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.

- Maximum Risk Background Check: For a contract worker requiring a maximum 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, identity theft, computer fraud or abuse, and embezzlement.
- e. If a contract worker has a criminal record that includes a disqualifying conviction, that person will not be permitted to perform work for the City under the contract.
- f. If the records check indicates that the disposition of the criminal case is unknown, the contractor must determine the disposition.

C. CONTRACTOR REQUIREMENTS

1. The contractor will require a Contract Worker Disclosure for each contract worker who is performing work for the City, which will be made available to the City upon request. The contractor will also be responsible for obtaining a background check required by this AR on every contract worker that will be assigned to work for the City.
2. In the Standard category, the contractor will be responsible for reviewing the results of the background check, and deciding if any contract worker should be disqualified for work under a City contract pursuant to the criteria set forth in this Section IV, Evaluating Results. The contractor is required to engage in whatever due diligence is necessary to make the decision on whether to disqualify a contract worker. Once the contractor has decided, the list of names of qualified contract workers will be submitted to the contracting department.
3. For sole proprietors, the Contractor must comply with the background check for himself and any business partners, or members or employees which will assist on the contract and for whom the requirements of this AR apply.
4. In the Maximum category, the contractor will perform the same review as required in the Standard category. However, when submitting the list of qualified contract workers, the contractor will also submit the results of the background check to the contracting department. If, upon review of the information submitted, the City advises the contractor that it believes a contract worker should be disqualified, the City will notify the contractor of that fact, and the contractor will reevaluate the contract worker to determine whether the person should be disqualified. If the contractor believes that there are extenuating circumstances that suggest that the person should not be disqualified, the contractor will discuss those circumstances with the contracting department. The contracting department decision will be considered final.

D. CONTRACT LANGUAGE

The following types of provisions may be recommended in all contracts requiring background checks on contract workers:

- A provision requiring a contractor to acknowledge the City may require a background or security screening of the contractor's workers be conducted by the contractor.
- A requirement that the contractor, after obtaining the results of a background check, will determine if the background check results contain any potentially disqualifying factors, and allow those contract workers to work under the contract who do not have disqualifying factors in their record.

- Contract worker maximum or Criminal Justice Information System (CJIS) background check will be valid for whichever is shorter, the contract term or three years.

E. DEPARTMENT COMPLIANCE

Each department is responsible for complying with the requirements of this AR; non-compliance may be considered a violation of the Procurement Code.

F. VARIANCES AND EXEMPTIONS

1. There are federal and state regulations that necessitate an exemption from this policy. Contract workers who fall under these areas may be considered exempt from this policy, as well as other acceptable evidence of an existing background check or clearance:
 - Federal Homeland Defense Bureau (e.g. Aviation, Water Services, Transit, Police and Fire Departments).
 - Transportation Security Administration (e.g. Aviation, Fire, and Police Departments).
 - Federal Aviation Administration (e.g. Aviation, Police, and Fire Departments).
 - Department of Public Safety (DPS) Administration – presenting a current Level One Department of Public Safety fingerprint card (e.g. Human Services, Housing, Parks, and Aviation Departments).
 - Arizona or other State Bars (Lawyers registered to practice and licensed by a State bar).
 - Existing evidence of a background check performed within the last 3-5 years may be approved by the authorized department, if the contract worker's background check fits all required criteria herewithin.
2. Any variance from this policy is to be reviewed and approved by the Security and Access Review Committee.

G. AUDITING AND PROCESS REVIEW

1. Departments will perform regular Contract Worker Disclosure audits and process reviews per prescribed City guidelines in conjunction with the implementation of this AR. The City Auditor Department may also perform audits as it deems necessary.
2. Violations of this AR may result in disciplinary action up to and including termination.

H. QUESTIONS

Questions regarding this AR should be directed to the Public Works Department Badge Imaging Office at 602-534-4611.

ED ZUERCHER, City Manager

By Toni MacCarone
Toni MacCarone,
Acting Deputy City Manager

LEVELS OF ACCESS GUIDE

This table can be used as a guide in determining what type / level of access is needed in an area.

Exposure Type	Potential Target	Risk	Security Risk Level	Typical Features	Security Requirements
Theft of tools, equipment, computers, Petty cash, & other low value assets (<\$5,000).	Shops Warehouses Storerooms Cash drawers General office areas	(1) Small monetary loss (2) Loss of low value assets	Standard Risk Level	Partially secure - area is not secure but identification system makes detection likely. Badging & Key Control Systems Effective Administrative Controls. *	(1) Identity of person entering area should be known and verifiable. (2) Person entering must have a demonstrated and approved need for access. (3) Public must be escorted by a City employee.
Violence, Irrational Behavior	Employees of the City Elected officials	(1) Injury or death (2) Loss of employee confidence	Standard Risk Level or Maximum as applicable**	Partially secure - area is not secure but identification system makes detection likely. Badging & Key Control Systems Effective Administrative Controls. *	(1) Identity of person entering area should be known and verifiable. (2) Person entering must have a demonstrated and approved need for access. (3) Public must be escorted by a City employee.
High Value Theft (> \$5,000)	Servers, Databases, Money Rooms Equipment	(1) Large monetary loss (2) Loss of valuable assets (3) Public criticism	Maximum Risk Level	Very secure – physical barriers surround areas that are very difficult to breach. Any breach would be detected. Badging & Key Control Systems Effective Administrative Controls. * Card Readers at all entry points.	(1) Identity of person entering area should be known, verifiable and documented. (2) Person entering must have a demonstrated and approved need for access. (3) Public must be by escorted a City employee.

<p>Data Theft Infrastructure Attack</p>	<p>Data processing centers Billing Centers Water plants Communications centers Infrastructure Elections Areas HIPAA or State or federally mandated to protect HAZMAT areas</p>	<p>(1) Substantial business interruption (2) Substantial damage (3) Substantial monetary loss (4) Public criticism and lack of confidence (5) Fines and liability (6) Terrorism (7) Catastrophic Loss (8) Injury and death (9) Loss of public's sense of security</p>	<p>Maximum Risk Level</p>	<p>Completely Secure – formidable physical barriers surround areas that are virtually impossible to breach. Any breach would be detected. Badging & Key Control Systems Effective Administrative Controls* Card readers at all entry points Record of persons entering- identity, date and time Video surveillance at entry points</p>	<p>(1) Identity of person entering area should be known, verifiable and documented (2) Persons entering have had a background check with a high level of scrutiny. (3) Approval of access must be by a functional head of the facility or restricted area. This authority cannot be delegated. (4) All breaches should be detected and investigated (5) Access lists must be established and audited frequently (such as monthly or quarterly).</p>
<p>Children and Vulnerable Adults</p>	<p>Children, <i>Vulnerable Adult</i> means an individual who is eighteen years of age or older who is unable to protect himself from abuse, neglect or exploitation by others because of a mental or physical impairment Children and Elderly programs, and other Specialty programs where direct contact with these populations occur</p>	<p>(1) Public criticism and lack of confidence (2) Injury and death (3) Loss of public's sense of security</p>	<p>Maximum Risk Level</p>	<p>Very secure – physical barriers surround areas that are very difficult to breach. Any breach would be detected. Specialized Systems, Badging & Key Control Systems Effective Administrative Controls</p>	<p>(1) Per City Code 2-27; City Ordinance (formerly PCC 2-45.6 - Ord. No. G-5047, 1, Adopted 12-19-2007, eff. 1-18-2008) (2) Per ARS Section 46-141</p>

*Effective Administrative Controls include – designated administrator, clear policies & procedures stating importance of system, employees required to challenge unbadged persons & report infractions, tailgating prohibited (letting others into an area without requiring them to use their access badge), periodic audits & inspections, reliable inventory system for badges & keys, and appropriate penalties for violations of policy, and ongoing maintenance of systems, policies, etc.

** Person interacting with Elected Officials or directly working in elected official areas.