QDC MONITORING SERVICES, LLC
3141 Fairview Park Drive
Suite R-95
Falls Church, VA. 22042
(O) 703-641-8900
card-admin@quad1.com

QDC Monitoring Services, LLC (Solution Center) has been retained by the building management to provide access control services for the base building perimeter doors and elevator access at the following locations:

- 8000 Towers Crescent Drive
- 8010 Towers Crescent Drive
- 8020 Towers Crescent Drive
- 1850 Towers Crescent Plaza

Equipment installation work is currently underway and should be completed by the second week of January 2012. The Solution Center will begin providing card administration services, alarm monitoring, remote access, and after-hours emergency answering services effective January 1st, 2011 for the buildings. The transition to the Solution Center will not impact individual tenant's access control equipment or services. Tenants will continue to contract with their own 3rd party access control vendors, or maintain their own in-house access control services for their tenant suite doors if applicable. The buildings will continue to follow the same time schedule that the doors and elevators are now secured and unsecured unless otherwise instructed by management.

Attached is the card administration form that should be used when submitting card requests to the Solution Center. The official conversion date is scheduled for January 1, 2012, but in order to capture revisions to tenant's card holder lists, please begin forwarding card requests to the Solution Center effective immediately. The card administration form is created in an Excel format spreadsheet. When using the form, please refrain from using color background or font since the forms are printed in black and white. The attached card administration form has been completed as an example which can be edited for your appropriate companies. If there are any questions pertaining to the submission process, or how to complete the form correctly, please do not hesitate to contact me at 703-641-8900. On a separate note, please do not send card requests in the context of emails. On numerous occasions, the request becomes an email chain letter, and these types of card request become difficult to decipher and may result in unnecessary mistakes. An email with the card administration form as an attachment is the ideal suggestion for a card request.

Card requests can be forwarded via email to card-admin@quad1.com. Upon receipt, card requests will be processed in most circumstances within a twenty-four (24) hour period during normal business hours. Tenants will receive email confirmation that the request was completed by the Solution Center personnel. **Please note that tenants will be required to send card administration requests to their individual 3rd party access control vendors for their own individual tenant suite doors**.

Since the Solution Center wants to be certain that we are processing authorized card requests per the tenant's approval, the Solution Center will only accept and process card requests from designated tenant appointees. This will prevent individual employees from attempting to submit unauthorized card requests, and the assurance of maintaining an accurate card holder databases for each company.

There are four (4) card action requests on the card administration form which are explained below in further detail. In order to make sure a specific request is handled correctly and without confusion, please refrain from ad libitum phrases such as, DELETE-CANCEL-ELIMINATE-ERASE.

I. **A – Activation Request:** Tenant has an inactive card in their overstock that they wish to activate for a user.

II. **D – Deactivate Request:** Tenant has received a card back from a user that was active but the user no longer needs the card due to resignation, termination, etc. The card will be listed with an "inactive" status, and remain in the database as an inactive spare card for future distribution. If an employee returns a card because it no longer works then it would be a REMOVE request, and the card/fob should be discarded as non-operational. See remove request definition.

III. **R – Remove Request:** Tenant is requesting that the card be removed from the database since it's become defective, lost, stolen, or the user left the company but did not return the card to the tenant's overstock. This request removes the card number out of the database since the tenant will no longer be issuing the card/fob to another employee.

IV. **U – Update Request:** Tenant is requesting that the card holder's information has been changed. Card has been issued from one employee to another employee, access level may change, surname change, etc.

Additionally, the access levels that were created provide an employee with access into the building on a 24x7x365 basis. Each tenant has their own access level which permits access through the base building perimeter doors, garage elevator lobbies, and elevator access to the tenant's appropriate floors.

The access levels in our system are entered in a standard format for each tenant. Basically, the access level is the numerical address of the building which is then followed by the tenant name, i.e.

I. **8000 RSM McGladrey**
II. **8010 Targus Information**
III. **8020 Capital One**
IV. **1850 MicroStrategy**

Please note that the Solution Center is able to customize access levels to fit the requirements for each tenant. For example, a tenant may have an employee/consultant which they want to restrict access to the building during certain hours. We can set-up an access level which allows an employee access into the building during the week but not during the weekend or holidays. The new access level would be listed in a description similar to the access level noted below.

8000 RSM McGladrey B'Ness Hrs

Also, included for your review is the "After Hours Remote Building Access" policy utilized by the Solution Center. It would be advisable to have tenants' employees become familiar with the policy to negate any confusion or unfavorable discourse between the Solution Center personnel and a tenant's employee. Solution Center operators are trained and instructed to closely adhere to the policy when providing remote access into a building to insure a level of security to building occupants and their property. The Solution Center doesn't want to permit entry into a building to just anyone for the safety of all tenants.

In conclusion, the Solution Center is a separate licensed and insured entity of QDC Management Services, Inc. It is a full service after hours emergency dispatch center, providing access control monitoring, installation, and R&M contracting services. It is operated by Quadrangle as a tenant enhanced service, and as an alternative to other outside 3rd party access control vendors. The Solution Center operates with the underlined business principle that clientele shall receive the special attention and quick response that you may not receive from some of our competitors. If you feel that your access control services, or after-hours answering service requirements are not being satisfactorily fulfilled, or you'd like to receive a competitive cost estimate for any access control requirements that you may have now or in the future, please retain my information on record, and I'd be more than happy to assist you should the need arise.

Thank-you in advance for your time and consideration. Again, if you should have any questions or concerns, please do not hesitate to contact me at your convenience.

Sean O'Leary, Director of Operations
QDC Monitoring Services, LLC
3141 Fairview Park Drive, Suite R-95
Falls Church, VA. 22042

(O) 703-641-8900 (F) 703-876-5733
soleary@quad1.com

AFTER HOURS BUILDING REMOTE ACCESS POLICY

All tenant and building employees are issued access proximity cards/fobs or insert keys to gain entry into a building when the site is in the locked down mode, usually during non-business hours, weekends and holidays. The cards or keys are activated upon the request of a building tenant. Cards or keys will contain the user's name, card/key number, access level, card status, tenant name and building address. The card or key information is stored in the databases of both Honeywell access control front end systems located in the Solution Center. If a person's access card or key is active in the access control system(s) then the person's information will be on record and that person is authorized to enter the building. If a person's access card is de-active in the access control system then that person's information may be on record but that person will not be allow access into the building. **Only individuals with ACTIVE cards or keys will be permitted access into a building.**

When a building is secured, any person wishing to gain entry into a building must use an access card or insert key. If an individual is not in possession of an access card or key, or there is no record of the person in the Honeywell access control system then **AT NO TIME shall Solution Center personnel permit access into a building by remotely "pulsing" the door open via the access control system.** Politely explain to the individual that it's against building security policy to allow anyone access into a building that does not have a card or key, or whose information is not on record.

THE ONLY TIME that personnel may grant an individual access into a building when the person is not in possession of their access card is when the person can correctly furnish ALL of the following four pieces of information. 1. Access Card Number 2. Cardholder's First & Last Name 3. Cardholder's Company Name 4. Building Address. But before granting access into a building, first the Solution Center operator **MUST** verify that the information provided by the person identically matches the cardholder's record in the Honeywell front-end system and secondly, that the cardholder's card or key number is active in the access control system. When a person furnishes the correct information then the operator may provide access into a building. If any information provided by the individual does not match the information in the database, or there is no card record in the database, or the person does not have a card or key in their possession then the policy is **"NO ACCESS INTO THE BUILDING, NO EXCEPTIONS!"**

If the person is in possession of a card or key that is defective, non-functional, or the number of the card/key is not in the Honeywell system(s) and the person becomes abusive or irate, calmly inform them that you are only following company policy, and thereafter, instruct the person to report the problem to their company office manager, or card key administrator so the appropriate individual(s) can investigate and remedy the problem.

As a courtesy, when a person claims to be an employee of a building tenant but they are not in possession of their card or key, or they can not correctly provide the four pieces of information noted above, the operator should ask the person if they can provide the telephone number of a co-worker in the building who the operator can call to see if the co-worker will escort them into the building. If a operator calls a co-worker for the individual wishing entry, the operator must record on their Phone Log the name of the employee requesting access, and the name and phone number of the co-worker who escorted the person into the building as well as the time and date, address of the building, and the company name where the individuals work.

If the person requesting entry into a building is a visitor or guest, the operator shall request the name of the visitor as well as the name, telephone number, and company name of the person that the individual is visiting. The operator shall inform the visitor that they will attempt to contact the tenant employee via the telephone. Upon contacting the tenant employee, the operator shall inform the tenant that they have a visitor, and request that the individual go down to greet and escort the visitor into the building. You should have the door location available for the tenant so they'll know which door to greet their visitor. If the tenant is not available, or doesn't answer the phone then leave a message on that person's voice mail. At minimum, the message should provide the operator's name and call back number, as well as the visitor's name, time and date that the visitor arrived at the site, and any other pertinent information. If you do contact the person then record the name of the visitor, date and time as well as the name and phone number of person who escorted the person into the building, and the building address and company name where the individual works on your Phone Log for that particular call.

Under limited situations when a tenant has scheduled a special after-hours activity (seminar, meeting, construction work, etc.), and the tenant notifies the property management office in writing, and furnishes them with the names and date and times of the event, the Solution Center personnel will provide access into the building only for those names that are posted on a list. Again, this is the exception and not the norm since the Solution Center personnel can not truly verify who they are providing remote access. It should be the responsibility of the tenant to furnish after hours access for their guests and vendors.

In addition, operators shall **NEVER** open or provide access into a tenant's leased space to anyone, nor shall the operator ever enter the tenant's space without prior authorization from the property management staff for that particular building. In instances that require entry into a tenant's suite for abnormal or emergency conditions such as fire or

medical emergency, the operator will immediately notify the Property Manager of the building, who'll in turn notify the tenant.