# PRIVACY POLICY

**For: BCI PROPERTIES, LLC**
**Staff, employees & vendors**
**Updated: 4-18-09**

"Personal information" means any combination of the consumer's name, social security number, drivers license number, passport number or financial account, credit card or debit card numbers which would be sufficient to permit identity theft. Confidential information includes any information regarding a tenant/applicant that is required by law to be kept confidential.

I. Administrative safeguards

A. Responsible persons: the Portfolio manager and site manager. At this time those people are Donald J. Leske II (Desig/Broker) and Emily Leske (Licensed Agent).

B. Foreseeable risks:

1. Access to computer and hard copy files by unauthorized persons both on-site and at the home office

2. Remote computer access

3. Fax and electronic transmittal of confidential information

4. Release of confidential information to unauthorized third parties

5. Resident access to on-site fax/copy machines/computers

6. Access to tenant files, information maintained in files

7. Loss of portable computer storage devices

8. Lock Out assistance, if allowed who has individual access to keys/units

9. Access to confidential information in tenant's units during repair/inspections

10. Security of on-site office, who has access

11. Access to storage of dead files

12. Disposal of dead files

13. Access to drop box by unauthorized persons and secure from break-ins

C. Annual assessment of risks and safeguards in place to control the risks

D. Training and managing personnel:

1. New personnel: immediate policy review and training. Personnel sign acknowledgement of policies receipt and agreement to abide by the policies

2. Existing personnel: annual review of policies and signing of acknowledgement of policies receipt and agreement to abide by the policies

3. Specific consequences for violation

E. Selecting service providers capable of maintaining appropriate safeguards

II. Technical safeguards

A. Assessing risks in network and software design

1. Work with network consultants to ensure network security is kept updated and in house measures

2. Work with network consultants to ensure remote access security is kept updated
Does company host service of own computers / off site virtual.

b) Is system hosted off-site, security of providers system

3. Determine if there are any portable media drives on which information which is stored.

4. Scanners –
Protection of information

b) After scanning, what happens to information / eyes only PC is password protected.

5. Establish protocol for personal information sent in emails

6. On-line rent payments
a) both ends of transaction encrypted

7. Credit card payments
Receipts using truncated numbers

b) last four digits of credit card appearing on customer copy

B. Information processing and transmission

1. Upon transmission of application to screening company safeguard application
Separate file for pending applications maintained in locked location

Once file is completed it is put in a locked file box, on site

2. Confirmation of fax number or email address accuracy prior to transmission

C. Detecting, preventing and responding to attacks

1. Detection: work with computer consultants to have system in place for immediate detection of unauthorized access

2. Prevention

a) Computer passwords must be a combination of letters and numbers and must be changed every four months

b) Desktop computer passwords must never be released to unauthorized third parties

c) Desktop computers - screensaver with password protection automatically comes on after 10 minutes idle

d) Network logins and passwords must never be released to third parties or personnel who are not authorized for network administration

e) Employee network access must be immediately removed upon termination of employment

f) Remote access:

(1) User must ensure confidential information is not visible to unauthorized parties

(2) User must not leave the computer while still logged in when unauthorized parties are present

(3) User must log off immediately when remote login use is completed

3. Response
    Immediate change of login and passwords for all computers
    Immediate assessment of files accessed
    Immediate notification of consumers (tenants or applicants) if information was accessed

D. Regular testing: monthly network assessment and maintenance

III. Physical safeguards

A. Assessing the risks of information storage and disposal

1. On-site access to hard copy files by:
    Visitors
    Property management company staff

Janitorial service providers
Service providers hired by Apartment Complex/Management Company including providers of plant services, office equipment repair, computer consultants, and coffee services / all Licensed & Bonded

Temporary/contract employees

Former employees

2. Access to documents disposed of

3. Access to on-site storage

4. Access to off-site storage

5. Access to drop box and secure against break in

6. Improper disposal of confidential information by Apartment Complex/Management Company personnel

7. Improper disposal of confidential information by shredding company

8. Off-site transport by personnel of hard copy and computer files

B. Detecting and preventing intrusions

1. Detecting:
a) Run card access log to determine who has entered office at what times
b) Check computer history
c) Alarm monitoring verify if has been on/off, and if off for what purpose

2. Preventing:

. All prospective tenants must complete guest card and provide photo ID when touring property
. Property management company/apartment complex staff must sign a confidentiality agreement that their staff and contractors will not read files or documents (except as necessary for their job functions) and will not release any confidential information
. Janitorial company must sign a confidentiality agreement that their staff and contractors will not read files or documents and will not release any confidential information
. All contractors hired by apartment complex/management company must be licensed, bonded and insured. Sign agreement that their staff and contractors will not read files or documents and will not release any confidential information, including any information seen in a tenant's unit
. Immediate return of keys and key card, and change of front door lock and back door code upon personnel termination
. Access to on-site and off-site storage limited to authorized Apartment Complex/Management company personnel

g) All file cabinets locked at night. Access to files be kept to minimum of employees

h) Drop box designed to prevent break ins

i) Off-site transport of hard copy and electronic files:

(1) Electronic and hard-copy files and computers stay in personnel's possession at all times

(2) Electronic and hard-copy files and computers never left in a vehicle

(3) Computer security (password, screensaver lock and encryption?)

(4) Secure off-site storage of back-up tapes

C. Implementing proper disposal methods.

1. All documents with any information related to tenant files must be shredded and properly disposed of by management company personnel or placed in the shredding bin for a shredding contractor to dispose of
2. Shredding contractor must sign agreement of confidentiality and certify use of proper disposal methods

---