



Technology and Information Systems Policy

OPERATIONS

OPERATIONS

VERSION
1.0

EFFECTIVE
March 2026

REVIEWED
March 2026

POLICY

This policy is to ensure that all technology, information systems, and digital resources used in the management of Barkan client properties are secure, properly maintained, and used exclusively for legitimate business purposes. This policy establishes standards for account ownership, password management, IT service arrangements, acceptable use, and compliance oversight. This policy applies to all Barkan property managers, general managers, employees, contractors, and third-party vendors who access or manage technology, accounts, or data for Barkan client properties.

Ownership of Accounts and Records

1. All accounts, logins, contracts, domains, emails, licenses, subscriptions, installation media (e.g., CDs), and maintenance agreements must be established in the name of the client (e.g., Waterview Condominium Trust or Waterview Apartments).
2. All related documentation must be organized and stored in a locked, secure file located in the management office. This file must include:
3. A written record of all current passwords for accounts, services, routers, domains, and video systems.
4. Master codes for the key safe and other non-IT equipment.
5. These records must not be held exclusively by an IT consultant or employee.

Password Management

1. The secured file noted above is the only acceptable location for written password storage.
2. Passwords must never be written on notes, "post-its," or other unsecured materials.
3. Password manager software (e.g., LastPass) is strongly recommended for daily use.
4. Property Managers are responsible for ensuring that all written records are updated promptly when passwords change or new accounts are created.



Ownership and Use of Equipment

1. All computer equipment, software, subscriptions, and email accounts are the property of Barkan's client and must be used exclusively for legitimate business purposes.
2. Client email accounts must not be used for personal communication, online shopping, newsletters, or other unrelated activity.
3. All employees or positions should have their own login for software and should not share login or password information among users.

Technology Maintenance and IT Services

1. Each property must maintain a calendar of renewal dates for all subscriptions, including antivirus, Office 365, domain registrations, backups, etc.
2. Each property must have a professional, third-party IT services agreement. This work must not be performed by residents or Barkan employees. Barkan's corporate IT vendor cannot provide these services.
3. Preventative maintenance visits should be scheduled twice per year, with additional support available on-demand either in person or through remote tools.

Brand Representation

1. Property Managers must ensure that email footers, voicemail recordings, and other public-facing communications align with Barkan brand guidelines (exhibit).

Responsibilities of Management

1. Property Managers and General Managers are responsible for ensuring that all employees:
 - a. Understand Barkan's policies regarding technology, information privacy, and acceptable use.
 - b. Comply with these policies in daily practice.
 - c. Managers must monitor compliance and take disciplinary action for violations.
 - d. All violations must be reported to the supervising Account Executive or Vice President.



Unacceptable Uses

1. The following are strictly prohibited and constitute grounds for immediate termination:
 - a. Using workplace equipment for harassment, discrimination, pornography, or intimidation of any kind.
 - b. Displaying sexually explicit materials.
 - c. Using offensive, abusive, or vulgar language.
 - d. Engaging in unprofessional, inappropriate, excessive, or disruptive use that interferes with business operations.
 - e. Sending or forwarding chain letters, spam, or broadcast emails.
 - f. Soliciting outside business ventures, political, or religious causes.
 - g. Disclosing confidential or proprietary information (including financial records, employee information, databases, access codes, or business partnerships) without prior company authorization.
 - h. Transmitting copyrighted or proprietary materials in violation of federal or state law.
 - i. Installing or using unlicensed software.

For additional information, please refer to the site tech guide (exhibit).