INFORMATION SECURITY POLICY

May 28, 2024

Capstone Tropical Holdings, Inc.

Capstone Title, LLC

Tropical Realty & Investments, Inc.

DBA. Berkshire Hathaway HomeServices Florida Properties Group

CAPSTONE
TROPICAL HOLDINGS

CAPSTONE
TITLE

BERKSHIRE
HATHAWAY
HOMESERVICES

FLORIDA
PROPERTIES
GROUP

Table of Contents

1. Policy Statement and Information 2
2. Risk Management 3
3. Data Classification 3
4. Access Control 4
5. Physical and Environmental Security 5
6. Operations Security 7
7. Communications Security 10
8. Incident Response 11
9. Business Continuity Management 12
10. Roles and Responsibilities 12
11. Compliance 13
12. Policy Review and Update 13

1. Policy Statement

This document outlines the protection of information assets within Capstone Tropical Holding, Inc., Capstone Title, LLC, and Tropical Realty & Investments, Inc. DBA, Berkshire Hathaway HomeServices Florida Properties Group

1.1 Purpose

This Policy's primary purpose is to establish a set of standards and guidelines that safeguard the confidentiality, integrity, and availability of data.

1.2 Scope and Applicability

This policy applies to all employees, contractors, and affiliates who interact with the organization's information systems. The scope of this policy encompasses all forms of data, whether digital or physical, that the organization owns or manages.

1.3 Objectives

By adhering to this policy, the organization aims to mitigate risks associated with data breaches, cyber threats, and other security incidents. It is applicable across all departments and units, ensuring a unified and consistent approach to information security. Compliance with this policy is mandatory for all stakeholders, as it is integral to maintaining the trust of clients and the reputation of the organization. Through this policy, the organization demonstrates its commitment to upholding the highest standards of information security.

1.4 Terms and Definitions

For the purpose of this document, the following terms and definitions apply:

a. **Asset.** Anything that has value to the organization.
b. **Control.** Means of managing risk, including policies, procedures, guidelines, and practices.
c. **Guideline.** A description that clarifies what should be done and how.
d. **Information Security.** Preservation of confidentiality, integrity, and availability of information.
e. **Policy.** Overall intention and direction as formally expressed by management.
f. **Risk.** Combination of the probability of an event and its consequences/
g. **Third Party.** A person or entity that is recognized as being independent.
h. **Threat.** Potential cause of an unwanted incident which may result in harm to a system.
i. **Vulnerability.** Weakness of an asset that can be exploited by one or more threats.

2. Risk Management

2.1 Regular review and update of risk assessments.

Formal organization-wide risk assessments will be conducted by the organization no less than annually or upon significant changes to the organization environment.

2.2 Process for identifying, evaluating, and addressing risks.

a. Risk assessments must account for administrative, physical, and technical risks.
b. Information security risk management procedures must be developed and include the following (at a minimum):
    i. Risk Assessment
    ii. Risk Treatment
    iii. Risk Communication
    iv. Risk Monitoring and Review
c. Risk evaluation criteria should be developed for evaluating the organization's information security risks considering the following:
    i. The strategic value of the business information process.
    ii. The criticality of the information assets involved.
    iii. Legal and regulatory requirements, and contractual obligations.
    iv. Operational and business importance of availability, confidentiality, and integrity.
    v. Stakeholders' expectations and perceptions, and negative consequences for goodwill and reputation.
    vi. All risks will be classified and prioritized according to their importance to the organization.
    vii. Periodically, the organization may contract with a third-party vendor to conduct an independent risk assessment and/or to validate the effectiveness of the organization risk management process.

3. Data Classification

3.1 All employees and other covered individuals are responsible for:
a. Understanding what constitutes Private or Public information; and
b. Managing Private or Public information in a manner consistent with the criticality of and the requirements for confidentiality associated with the data in any form (electronic, documentary, audio, video, etc.) throughout the entire information lifecycle (from creation or acquisition through preservation, storing or disposal).

3.2 Classification Levels

All information whether at rest (i.e., stored in databases, tables, email systems, file cabinets, desk drawers, etc.) or in use (i.e., being processed by application systems, electronically transmitted, used in spreadsheets, or manually manipulated, etc.) must be classified into one of the three data classification levels.

a. Determining classification level should be done according to an assessment of the need for Confidentiality of the information.

Confidentiality: Access to information must be strictly limited to protect the organization and individuals from loss.

Limiting access to authorized individuals/entities/devices ensures legal obligations are fulfilled and/or protects the organization and its stakeholders from the disclosure of data which is sensitive in nature.

Note: The appropriate classification of each data set is based on the classification of the most confidential data stored in the data set (e.g., the database, table, file, etc.), or accessed by systems or people. This is true even if the data set contains other information that would qualify for a lower level of protection if it were stored separately.

b. The table below summarizes the Data Classification process. All individuals covered under this policy are required to handle information per the procedural controls of each department.

i. **Level I – Confidential Information**: High risk of significant financial loss, identity theft, legal liability, public distrust, or harm if this data is disclosed.
ii. **Level II – Sensitive Information**: Moderate requirement for Confidentiality and/or moderate or limited risk of financial loss, identity theft, legal liability, public distrust, or harm if this data is disclosed.
iii. **Level III – Public Information**: Low requirement for Confidentiality [information is public] and/or low or insignificant risk of financial loss, identity theft, legal liability, public distrust, or harm if this data is disclosed.

4. Access Control

4.1 User Access Management

a. Access to systems and resources must be authorized by the appropriate manager.
b. Users must only have access to the systems and resources necessary for their job function.

4.2 User Responsibilities

a. Users are responsible for all actions taken with their user accounts.
b. Users must not share their access credentials with others.

4.3 Access Control Measures

a. The Organization will implement technical measures to control and monitor access to our systems and resources.
b. These measures may include, but are not limited to, user authentication, access logs, and intrusion detection systems.

5. Physical and Environmental Security

5.1 Area Security

a. Secure Areas - Physical Security Perimeter

i. Effective physical security measures help protect against unauthorized access, damage, or interference in areas where critical or sensitive information is prepared or located, or where information processing services supporting key business processes are hosted.
ii. The requirements and placement of each physical security barrier should depend upon the value of the information or service being protected.
iii. Each level of physical protection should have a defined security perimeter, around which a consistent level of physical security protection is maintained.

iv. Physical information processing resources that support key business processes in a production mode, (i.e., mainframes, minicomputers, etc.) must be housed in a secure area that reasonably protects the resources from unauthorized physical access, fire, flooding, explosions, and other forms of natural or man-made disaster.
v. Managers responsible for sensitive information or for information processing resources should periodically perform an assessment to determine the existing level of security vulnerability and compliance with the physical security requirements.

b. Physical Entry Controls

i. It is the responsibility of the Organization to enforce entry controls and authentication procedures that ensure that only authorized personnel are allowed entry into areas that house critical or sensitive information or information processing resources that host the processing of critical or sensitive information (i.e. information processing centers).
ii. Personnel should be encouraged to question the presence of unauthorized personnel. Visitors should be escorted into areas where equipment owned by the Organization can be used to access network resources restricted for use by its staff and agents.
iii. The distribution of keys or passes (including ID badges, card/pass keys, and entry codes) used to physically access secure areas must be strictly controlled and subject to frequent review to ensure that only currently authorized individuals are in

possession of access devices. Quarterly reviews should be performed to ensure that only those individuals with a job-related need have access to the computing facilities. Whenever individuals change jobs or leave the Organization, their means of access should be removed immediately and any physical device used that belong to the Organization should be returned if applicable.

c. Clear Desk Policy

i. Departments should encourage employees to practice a clear desk policy for papers, storage devices, and other media that are sensitive in nature, to reduce the risks of unauthorized access, loss of and damage to information outside of normal working hours. The following guidelines should be applied, where appropriate:

i. Papers, storage devices, and other media should be stored in cabinets when not in use, especially outside working hours.
ii. Sensitive or critical business information should be locked away (ideally in a fire-resistant cabinet) when not required especially when the office is vacated.
iii. Personal computers, computer terminals, and other devices used for network access, should be protected by key locks, passwords or other controls when not in use. Consideration should be given to the need to protect incoming and outgoing mail points and unattended fax machines and printers.

5.2 Equipment Security

a. Removal of Property

It is the responsibility of management to enforce authorization and control procedures that ensure information-processing assets such as equipment or software are removed from the Organization's property for business purposes only.

Note: Removal of information and data is governed by its classification controls.

b. **Equipment Placement & Protection**

i. Information processing resources should be located away from hazardous processes or materials.
ii. Adequate power supplies and auxiliary power supplies should be provided to information processing resources.
iii. Adequate protection should be provided to information and information processing resources against damage from exposure to water, smoke, dust, chemicals, electrical supply interference, etc.
iv. The minimum-security protection activities specified by the vendor/manufacturer of information processing equipment must also be implemented.
v. Physical emergency procedures should be clearly documented. All personnel should be trained in appropriate behavior in emergencies.

c. Environmental

i. Air-conditioning units should be sufficient to support the equipment in computing facilities.

d. Fire Suppression

i. Both manually activated and automatically activated fire suppression equipment should be installed. As a safety measure, if the automatic fire suppression system employs water, power to the computer room should be automatically shut off prior to water release. The automatically activated fire suppression system should be inspected and tested annually.

ii. Self-contained portable fire extinguishers should be sufficient to ensure complete coverage. Fire extinguishers should be conveniently located, well-marked and inspected on a periodic basis.

b. Power Supplies

i. An Uninterruptible Power Source (UPS) should be used to support critical business information processing operations. UPS equipment should be regularly tested according to the manufacturer's recommendations. Computer hardware should be protected from electrical surges.

c. Cabling Security

i. Power and communications lines servicing buildings should be underground, where possible, or subject to adequate alternative protection. Network cabling should be protected from unauthorized interception or damage.

d. **Security of Equipment in Public Places or Off-Premises**

i. Virus controls must be enabled to protect all Organization resources.

ii. Information processing equipment and media containing highly restricted and confidential data should not be left unattended in public places. Portable computers containing sensitive data should be carried as hand luggage when traveling.

iii. Off premise computers with classified information should be protected with an appropriate form of access protection, e.g. passwords, smart cards, or encryption, to prevent unauthorized access.

iv. Manufacturers' instructions regarding physical protection of equipment should be observed at all times.

v. Security risks (e.g. of damage, theft, eavesdropping) vary considerably between locations and should be considered in determining the most appropriate security measures.

e. **Secure Disposal of Equipment**

i. Minimum guidelines should be established for removing ("wiping") the hard drive of computing equipment. If this is contracted to a vendor, a certificate of destruction should be provided.

ii. All equipment containing storage media, e.g., fixed hard drives, should be checked to ensure that any classified information and licensed software are removed or over written prior to disposal.

iii. Damaged storage devices containing information classified as restricted should be repaired or destroyed.

6. Operations Security

6.1 Documented Operating Procedures

a. Operating procedures shall be documented and made available to all users who need them.

6.2 Change Management

a. Changes to the organization, business processes, information processing facilities, and systems that affect information security in the production environment and financial systems shall be controlled by the Organization.
b. All significant changes to in-scope systems must be documented.
c. Change management processes shall include:
    i. Processes for planning and testing of changes, including remediation measures.
    ii. Documented managerial approval and authorization before proceeding with changes that may have a significant impact on information security, operations, or the production platform.
    iii. Advance communication/warning of changes, including schedules and a description of reasonably anticipated effects, provided to all relevant internal and external stakeholders.
    iv. Documentation of all emergency changes and subsequent review.
    v. A process for remediating unsuccessful changes.

6.3 Systems and Network Configuration, Hardening, and Review

a. Systems and networks shall be provisioned and maintained in accordance with the configuration and hardening standards.
b. Firewalls shall be used to control network traffic to and from the production environment in accordance with this policy.
c. Production firewall rules shall be reviewed annually.
d. Tickets shall be created to obtain approvals for any needed changes.

6.4 Protection from Malware

a. In order to protect the Organization's infrastructure against the introduction of malicious software, detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.
b. Anti-malware protections shall be utilized on all employee issued laptops except for those running operating systems not normally prone to malicious software. Additionally, threat detection and response software shall be utilized for the organization's email system. The anti-malware protections utilized shall be capable of detecting all common forms of malicious threats.
c. The organization should scan all files upon their introduction to systems, and continually scan files upon access, modification, or download.
d. Anti-malware definition updates should be configured to be downloaded and installed automatically whenever new updates are available.
e. Known or suspected malware incidents must be reported as a security incident.
f. It is a violation of the Organization's policy to disable or alter the configuration of anti-malware protections without authorization.

6.5 Information Backup

a. The need for backups of systems, databases, information, and data shall be considered and appropriate backup processes shall be designed, planned, and implemented.
b. Security measures to protect backups shall be designed and applied in accordance with the confidentiality or sensitivity of the data.
c. Backup copies of information, software and system images shall be taken regularly to protect against loss of data. Backups and restore capabilities shall be periodically tested, not less than annually.
d. The organization does not regularly backup user devices like laptops. Users are expected to store critical files and information in organization-sanctioned file storage repositories.
e. Backups are configured to run daily on in-scope systems.
f. The backup schedules are maintained within the backup application software.

6.6 Logging & Monitoring

a. Production infrastructure shall be configured to produce detailed logs appropriate to the function served by the system or device.
b. Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and reviewed through manual or automated processes as needed.
c. Appropriate alerts shall be configured for events that represent a significant threat to the confidentiality, availability or integrity of production systems or confidential data.
d. **Protection of Log Information**
    i. Logging facilities and log information shall be protected against tampering and unauthorized access.
e. **Administrator & Operator Logs**
    i. System administrator and system operator activities shall be logged and reviewed and/or alerted in accordance with the system classification and criticality.

6.7 Clock Synchronization

a. The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to network time servers using reputable time sources.

6.8 File Integrity Monitoring and Intrusion Detection

a. The organization’s production systems shall be configured to monitor, log, and self-repair and/or alert on suspicious changes to critical system files where feasible.
b. Alerts shall be configured for suspicious conditions and information technology staff shall review logs on a regular basis.
c. Unauthorized intrusions and access attempts or changes to the Organization’s systems shall be investigated and remediated in accordance with the Incident Response Plan.

6.9 Technical Vulnerability Management

a. Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities shall be evaluated, and appropriate measures taken to address the associated risk.
b. A variety of methods shall be used to obtain information about technical vulnerabilities, including vulnerability scanning and penetration testing.
c. External vulnerability scans shall be run on the production environment at least quarterly.
d. Interior vulnerability scans shall be run against test environments which mirror production configurations.

e. Additional scanning and testing shall be performed following major changes to production systems.
f. The IT department shall evaluate the severity of vulnerabilities, and if it is determined to be a critical or high-risk vulnerability, a service ticket will be created.
g. The organization assessed severity level may differ from the level automatically generated by scanning software or determined by external researchers based on the organizations internal knowledge and understanding of technical architecture and real-world impact/exploitability.
h. Tickets are assigned to the system, application, or platform owners for further investigation and/or remediation.
i. Vulnerabilities assessed by the organization shall be remediated in the following timeframes:

Determined Severity Remediation	**Time**
Critical	**30 Days**
High	**30 Days**
Medium	**60 Days**
Low	**90 Days**
Informational	**As needed**

j. Service tickets for any vulnerability which cannot be remediated within the standard timeline must show a risk treatment plan and planned remediation timeline.

6.10 Restrictions on Software Installation

a. Rules governing the installation of software by users shall be established and implemented in accordance with the organization's Information Security Policy.

7.0 Communication Security

Communications security is a critical aspect of information technology that ensures the protection and integrity of data in transit. Secure management of networks and data transmission involves various strategies and protocols to safeguard against unauthorized access and cyber threats.

7.1 Network Access and Management

a. External connections to the organization networks will be protected by a firewall.
b. Necessary network and security components shall be implemented, managed, and maintained in a secure manner.
c. All network and security components shall be configured to provide audit logs for necessary and continual security monitoring.
d. Confidentiality and integrity during transmission of critical data shall be ensured using appropriate encryption as required.
e. Access to the network components and security devices shall require strict access control and authentication as per the Access Control Policy.
f. Remote management of critical servers and network components shall only be done through properly encrypted channels.
g. All internet connection shall be passed through a content filtering solution to block undesirable web sites.

h. Appropriate network redundancy shall be built in the environment as per business requirements.
i. Detailed network architecture diagram shall be maintained up to date by the designated assignee in the Information Technology Department; and access to authorized users will be given on a need-to-know basis.
j. Required documentation in support of all activities, related to network and security components, shall be created, and maintained.

7.2 Remote Access

This policy sets the rules for employees and contractors who access the organization's network and resources remotely. It may include:

a. Approved remote access technologies (e.g., VPNs, remote desktop applications).
b. Authentication and encryption requirements for remote connections.
c. Device security guidelines (e.g., antivirus software, system updates, device encryption).
d. Restrictions on remote access locations and networks (e.g., prohibiting public Wi-Fi connections).
e. Procedures for revoking remote access privileges (e.g., when an employee leaves the organization).

7.3 Vendor Management

This policy aims to ensure that third-party vendors maintain appropriate security standards when handling an organization's information assets. It may include:

a. Criteria for selecting and evaluating vendors (e.g., security certifications, financial stability, past performance).
b. Requirements for vendor contracts (e.g., security clauses, confidentiality agreements, data ownership).
c. Vendor risk assessments and audits (e.g., reviewing security policies, testing security controls).
d. Procedures for monitoring vendor compliance and performance (e.g., regular reporting, incident response coordination).
e. Guidelines for terminating vendor relationships (e.g., secure data return or destruction, revoking access to systems, handling contractual obligations and penalties, post-contract reviews and lessons learned).

8.0 Incident Management

a. Information security incidents and vulnerabilities associated with information systems will be communicated in a timely manner. Appropriate corrective action will be taken.
b. Formal incident reporting and escalation will be implemented.
c. All employees, contractors and third-party users will be made aware of the procedures for reporting the different types of security incident, or vulnerability that might have an impact on the security of the organization’s assets.

d. Information security incidents and vulnerabilities will be reported as quickly as possible to serviceDesk@bhhsflpg.net or by contacting the help desk directly at 727-807-9696

9.0 Business Continuity Management

a. The organization will put in place arrangements to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.
b. A business continuity management process will be implemented to minimize the impact on the organization and recover from loss of information assets.
c. Critical business processes will be identified.
d. Business impact analysis will be undertaken for the consequences of disasters, security failures, loss of service, and lack of service availability.

10.0 Information Security Roles and Responsibilities

10.1 Executive Leadership

a. Oversight over risk and internal control for information security, privacy, and compliance.
b. Approves Capital Expenditures for Information Security and Privacy programs and initiatives.
c. Oversight over the execution of the information security and Privacy risk management program and risk treatments.
d. Communication Path to the Executive Leadership team
e. Aligns Information Security and Privacy Policy based on the organization's mission, strategic objectives, and risk appetite.

10.2 IT Manager

a. Oversight over information security in the software development process.
b. Responsible for the design, development, implementation, operation, maintenance and monitoring of development and commercial cloud hosting security controls.
c. Responsible for oversight of policy development.
d. Responsible for implementing risk management in the development process.

10.3 Systems Owners

a. Maintain the confidentiality, integrity, and availability of the information systems for which they are responsible in compliance with the organization's policies on information security and privacy.
b. Approval of technical access and change requests for non-standard access to systems under their control.

10.4 Employees, contractors, temporary workers, etc.

a. Acting at all times in a manner that does not place at risk the security of themselves, colleagues, and the information and resources they have use of and helping to identify areas where risk management practices should be adopted.

b. Adhering to the Organization's policies and standards of conduct reporting incidents and observed anomalies or weaknesses.

10.5 Human Resources

a. Ensuring employees are qualified and competent for their roles.
b. Ensuring appropriate testing and background checks are completed.
c. Ensuring that employees are presented with organization policies and the code of conduct.
d. Ensuring that employee performance and adherence to the code of conduct is periodically evaluated.
e. Ensuring, by working with the IT Manager, that employees receive appropriate security training and documentation of training is maintained.

11.0 Compliance

a. The organization will abide by any state or federal law, statutory, regulatory, or contractual obligations affecting its information systems.
b. The design, operation, use and management of information systems will comply with all statutory, regulatory, and contractual security requirements.

12.0 Policy Review and Update

a. The threat landscape, technology, and business environment are constantly changing. This policy is subject to regular reviews and updates to reflect the evolving nature of information security threats and technological advancements.