**SAFEGUARD PROPERTIES (Safeguard)**
**POLICY AND PROCEDURE MANUAL**

**POLICY: IT-SEC-POL-0140**
**SUBJECT: INFORMATION CLASSIFICATION POLICY**
**POLICY ADOPTION DATE: 02/24/2016**

Revision History

| Date | Version | Status | Comments |
|---|---|---|---|
| June 09, 2005 | 1.0 | Created | |
| August 24, 2009 | 1.1 | Updated | Updated company name (remove "INC.") |
| March 21, 2012 | 1.2 | Updated | Confidential definition to include 2 out of 3 rule |
| September 22, 2015 | 1.3 | Updated | Definitions brought up to date |

Document Control

| Role | Name | e-mail | Telephone |
|---|---|---|---|
| Author | Darren Kruk | darren.kruk@safeguardproperties.com | 216.739.2900 x3197 |
| Updater | Darren Kruk | darren.kruk@safeguardproperties.com | 216.739.2900 x3197 |

## I. POLICY

Information shall be classified according to its sensitivity and security requirements. These classifications shall be used with system-wide policies for ensuring appropriate security controls are implemented.

## II. PURPOSE

Ensure appropriate security controls are identified and implemented based upon the classification of information.

## III. GUIDELINES

All assets shall be classified according to criticality. Safeguard's information assets shall be properly inventoried, and classified in terms of their confidentiality, integrity, impact, sensitivity and criticality. Asset types include information, information systems, computers, and electronic storage media.

The Information Technology department shall maintain enterprise-wide inventories (registries) of assets. The designated owner of each information asset shall maintain accurate information about the asset, in the appropriate database.

All information under Safeguard's control shall be classified in terms of its sensitivity. This includes: electronic information, information recorded on paper, and information expressed orally or visually (such as by telephone, video conferencing). For classification purposes, Safeguard has defined four levels of sensitivity: Public, Private, Safeguard Restricted, and Confidential.

Information Systems

The designated owner of each Safeguard system is responsible for providing accurate and timely inventory information to the appropriate databases.

The System owner must ensure that the information that is created, received, stored and/or transmitted by the System has been accurately classified. If a System must handle Safeguard Confidential information, the System's security controls must meet the minimum baseline data protection standards for Safeguards Restricted information.

Each User of a System must be aware of the System's requirements for information handling and data protection.

Computers

The owner or administrator of each Safeguard computer is responsible for providing accurate and timely inventory information to the appropriate databases. This includes servers, workstations, laptops and other portable computers, and smartphones and other interactive electronic devices.

If a computer must be used to store Safeguard Confidential information, then the computer's location and its contents must be accurately tracked and documented at all times.

Legal

No attorney-client privileged communications shall be provided to any third party without the express written approval of Safeguard’s General Counsel.

Any request by any outside party for Confidential Information – either Client Information or attorney-client privileged communications – should be immediately directed to the Safeguard’s legal department.

No Client Information shall be provided to any third party without the client’s express written consent. Make certain to document all such requests.

Electronic Storage Devices and Media

If an electronic storage device or other digital medium must be used to store Safeguard Confidential information, then the location and the contents of the device or medium must be accurately tracked and documented at all times.

1. All information entered into, stored within, created by, reported from, or transported using Safeguard's computer systems is the property of Safeguard. Safeguard management reserves the right to observe and review activities of Safeguard computer users.

2. All Safeguard information must be classified as one of the following categories:

    - Confidential
    - Restricted
    - Private
    - Public

**Confidential**

Confidential Data is information that must be guarded due to proprietary, ethical, or privacy considerations and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute requiring this protection. Internal Data is information that is restricted to personnel designated by Safeguard management, who have a legitimate business purpose for accessing such data.

Description: Contains information whose unauthorized disclosure could cause severe damage to an individual or Client, or would be prejudicial to the interests of the Safeguard, (e.g. personnel or medical records, financial information, proprietary information, etc.). This includes Personally Identifiable Information, Payment Card Information, any financial or health information.

Distribution: Limited to employees who need to know it to perform their work.

This may be identified explicitly on each screen, copy, or listing by code letters meaning Confidential and an associated expiry date. Can affect not just the company's reputation to do business, but can filter down and affect our clients' reputation as well. They may be identified by the words (CONFIDENTIAL)

This classification of data must have the highest level of security and be guarded due to proprietary, ethical, or privacy considerations. It will be protected from unauthorized access, modification, transmission, storage or other use. Examples of Safeguard confidential data would include:

- Loan Number with relational aspect to other data
- Mortgagor Name (in combination with other personal data)
- Mortgagor Address (In combination with other personal data)
- Health Care Data (HIPAA)
- Payment Card Data (PCI)

- Employee specific information such as:
    - Payroll/401k/flex spending
- Educational Records (PIER)
- Driver's License number
- Attorney-client privileged communications, meaning, correspondence, phone-calls, documents of any kind, emails or any communication back and forth between Safeguard's attorneys – either in-house or outside counsel – and any Safeguard employee authorized to be dealing with or related to a pending legal, regulatory or litigation matter
- Any other data that may be considered PII or PCI

**Restricted**

Description: Contains information which itself, or in published form, has personal, technical or administrative sensitivity and is intended for internal use only, and should not be published or communicated externally except for official purposes. Examples would be certain correspondence, memoranda, procedures, minutes, contracts, etc. This may include HR documentation, security investigations, staffing plans or corrective actions.

Distribution: Those Safeguard employees who may need access to internal strategic planning, administrative or security investigations, Human Resource documentations such as PIP's and corrective action, and other such information.

This information is not made available to anyone outside of Safeguard Properties, Inc. with the exception of approved client requests. On occasion Safeguard will have to provide limited information to certain state and local regulatory bodies in connection with workers compensation or state qualification requirements. Sharing or disclosure of private information is provided exclusively by and through the Safeguard legal department. They may be identified by the words (RESTRICTED)

This classification of data will have the second highest level of security and be guarded due to proprietary, ethical, or privacy considerations. It will be protected from unauthorized access, modification, transmission, storage or other use. Examples of Safeguard Restricted data would include:

- Information that is received from clients of Safeguard i.e., loan information, work orders, and results of work orders ("Client Information") such as.
    - Loan Type (e.g. FHA, Conventional) in conjunction with other MBA data.
    - Client Name – in conjunction with other MBA data
    - Occupancy Status – in conjunction with other MBA data
    - Convey Date – in conjunction with other MBA data
    - Mortgagor Name (by itself)
    - Mortgagor Address (by itself)

- Financial data, pricing, business strategies, policies, and practices that may be exchanged between Safeguard and client.
- Contracts
- Financial reports/statements
- Business records ( Exec/Board meeting minutes, notes)
- SIRTs (Security Incident Response Tickets)
- Network Designs
- Software Code
- Strategic Planning documents

No company or client information shall be provided to any third party without the approval of executive management's consent. Make certain to document all such requests.

Any request by any outside party for Restricted Information – either client information or Safeguard Proprietary communications – should receive management approval before providing to the requestor.

**Private**

Description: Contains information that is public knowledge to Safeguard's employees, but should not be shared outside the company. This may include Safeguard proprietary information and processes that are intellectual property of Safeguard Properties. This includes information, which in electronic or published form, has technical or administrative sensitivity, and is intended for internal use only.

Distribution: Any Safeguard employee or internal contractor. Not to be published or communicated outside the company except for official purposes. They may be identified by the words (INTERNAL USE ONLY) at the discretion of the Owner, or if otherwise specified.

Examples of Safeguard PRIVATE data would include:

- General business reports
- Internal directories and organization charts
- Planning documents
- References
- Employee handbooks
- Performance review data
- General Benefits and health plan data and actions

**Public**

Description: Contains information which itself, or in published form, has no personal, technical or administrative sensitivity and is intended for global use, and may be published or communicated externally for official purposes. Examples would be marketing materials, website addresses, etc. All information may be found in public sources.

Distribution: May be published or communicated outside the company for official purposes. Items may be identified as public materials, marketing aides or similar documents.

- Information suitable for release to all Safeguard Properties employees and third party contractors and information approved by Marketing for general release to the public. Examples of public information include:
  - Public web pages
  - marketing materials
  - Publicly posted job announcements
- Disclosure of public data must not violate any pre-existing, signed non-disclosure agreements.

## IV. CLASSIFICATION PROTECTIONS

- When stored in an electronic format must be protected with a minimum level of authentication to include strong passwords, wherever possible.
- When stored on mobile devices and media, protections and encryption measures provided through mechanisms approved by the Safeguard Information Security Department must be employed.

## V. REQUESTS FOR CONFIDENTIAL OR PRIVATE INFORMATION

On occasion Safeguard will be required to provide information classified as Confidential or Restricted to certain federal, state, and local regulatory bodies or law enforcement agencies. Such requests include, but are not limited to requests or subpoenas from the OCC (Office of Comptroller of Currency), OIG, CFPG, Consumer Financial Protection Bureau, Internal Revenue Service ("IRS"), state or local Tax Authorities, the Department of Justice, FBI, or Child Support Enforcement Agencies. All requests by any outside party for Confidential or Private information of any kind shall be immediately directed to Safeguard's Legal Department.

Any request by any outside party for Confidential Information – either Client Information or attorney-client privileged communications – should be immediately directed to the Safeguard's legal department.

No attorney-client privileged communications shall be provided to any third party without the express written approval of Safeguard's General Counsel.

No Client Information shall be provided to any third party without the client's express written consent. Make certain to document all such requests.

## VI. RESPONSIBILITY

All Safeguard management will be responsible for implementing processes and procedures to meet the requirements set forth within this policy. It is the data owners' responsibility to classify their data in accordance with the Information Security Classification Policy.

## V. NON-COMPLIANCE

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. On-site contractors may have their access privileges terminated for failure to comply with this policy, up to and including termination of contract with Safeguard.