HAIGHT BROWN BONESTEEL, LLP

DATA PRIVACY POLICY

Effective Date	January 1, 2019
Current Version	1.0

I. OVERVIEW

Haight Brown Bone steel, LLP (hereafter "HAIGHT") computer systems and related applications (hereinafter "APPS") and devices collect and record activity for business purposes. This information should not be disclosed to unauthorized individuals.

II. PURPOSE

This policy declares the general privacy requirements for information automatically generated by APPs, computer systems, and network devices. The policy further delimits the conditions under which network data may be disclosed.

III. SCOPE

This policy applies to all who use HAIGHT Information Resources, including HAIGHT'S iCompCalculator.

IV. POLICY

A. NETWORK DATA

In the course of normal network operations, computer systems, voice systems, access control systems, and networks devices may automatically generate and track logging data, source and destination internet protocol (IP) addresses, session times, port numbers, file sizes, etc. (Network Data).

It is the general policy of HAIGHT to treat Network Data as private. This information may be obtained, stored, and reported for legitimate business purposes but shall not be exposed to unauthorized individuals except as specifically listed below.

B. EXCEPTIONS

Network Data may be exposed or disclosed under the circumstances listed below.

To maintain the integrity and availability of network operations. Network Data may intentionally or inadvertently expose Information Resources stored on networked machines or transmitted through the network in the following situations:

- Network performance monitoring or troubleshooting.
- Moving data through the network via automated store-and-forward systems.
- Copying, archiving, or otherwise preserving portions of messages transmitted over the network in the course of routine network maintenance activities.

In the event that messages or data files within the network indicate the presence of activities that violate internal policies or law.

In the event of recognized network security threats. HAIGHT reserves the right to investigate and remediate possible network security threats, including by means of capture, logging, and examination of files, communications, and other traffic and transmissions over or on the network.

In response to a court order.

In the event of a legitimate health or safety emergency.

In pursuit of reasonable business interests, such as fulfillment of partnership agreements.

C. REQUESTS FOR NETWORK DATA

All requests to retrieve and share Network Data must be submitted to the IT Department and must be approved by the appropriate Department head. Such requests shall include:

- Name and role of the requestor.
- Reason for the request, in accordance with the principles set forth in this policy.
- Intended use of the requested data.

Any network data intentionally shared with third parties must be sanitized to preserve the anonymity of network users.