Vocodia Information Security Plan

I. Objective:

Vocodia Holdings Corp's ("Vocodia") objective in the development and implementation of this information security plan is to create effective safeguards in order to protect our customers' non-public personal information. The plan shall evaluate our electronic and physical methods of accessing, collecting, storing, transmitting, protecting and disposing of our customers' non-public personal information.

II. Purposes:

a. Ensure the security and confidentiality of our customers' information;

b. Protect against anticipated threats or hazards to the security or integrity of our customers' information;

c. Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any of our customers.

III. Action Plans:

a. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or information systems;

b. Assess the likelihood and potential damage of these threats, taking into account the sensitivity of customer information;

c. Evaluate the sufficiency of existing policies, procedure and other safeguards in place to control risks.

IV. Action Steps:

a. Appoint a designated individual (or individuals) within the company to be responsible for:

   i. Initial implementation of this Plan;

   ii. Training employees regarding the Plan

   iii. Evaluating whether third party service providers maintain appropriate information practices that comport with this Plan

   iv. Periodic evaluations and adjustment to plan to ensure that it is still appropriate based on changes in technology, sensitivity of customer information, foreseeable internal/external threats, changes to business, and changes to customer information systems.

b. Train new employees regarding the Plan

c. Conduct Annual training session for employees and management regarding the Plan.

d. Determine reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or

information systems and evaluate sufficiency of existing policies and procedures for protecting such information.

V. Safeguards/Plan Policies:

a. Dissemination and training on the Plan

b. Employees encouraged to report any suspicious or unauthorized use of customer information

c. Require return of all customer information in former employee's possession

d. Eliminate access to customer information for former employees (change User ID/ passwords to log-in to computer system)

e. Prohibit employees from keeping open files or screens when stepping away from desk (notwithstanding working remotely as visitors could see screens)

f. Require all files to be secured at the end of the day, including logging out of computer

g. Have software that automatically logs user out after inactivity

h. Require periodic change of passwords for all employees

i. Use shredding machine to discard documents with customer information

j. In the event that company must discard obsolete computer hardware, must ensure secure disposal

k. Install firewall for access to company website

l. Instruct employees on protecting and securing removable devices that contain customer information

m. Install anti-virus software

n. Periodically update software

o. Evaluate third parties' systems if such third parties will have access to customer information