WHEREAS, the Board and Management desire to set forth clear roles, responsibilities and rule for the information technology network.

NOW THEREFORE, BE IT RESOLVED that the Lake of the Woods Association Board of Directors hereby adopts the Computer Security Policy as follows:

1.0 Purpose/Scope

The purpose of this policy is to define the roles and responsibilities and set forth the rules that govern the LOWA information technology network.

2.0 Activities Affected

All users of the LOWA information network including but not limited to:

2.1 Restaurant Management (Club House and Fairways)
2.2 Community Activity Management
2.3 Administration and Accounting
2.4 Communications (Channel 18, Lake Currents, Website, Member notifications)
2.5 Maintenance (Roads, Lakes and Common Area maintenance)
2.6 Security (Main and Rear gates, Cameras)
2.7 Golf course and Pro Shop
2.8 Site Connectivity and IT infrastructure (Data storage, printing, e-mail, Virtual Private Networks, and Internet Connectivity)
2.9 Other (Equestrian, Tennis, Fitness, etc.)

3.0 Related Documents and Forms

3.1 LOWA Employee Manual

4.0 Roles, Responsibilities, and Definitions

4.1 Roles and Responsibilities

4.1.1 Board of Directors- Oversee the greater expanse and provide foresight regarding the LOWA IT infrastructure. Approve various modules and large additions that may be purchased and installed. Adopt and periodically review broad policies for security of the computer network.

4.1.2 General Manager- Implements and enforces computer security policies, recommends policy changes to the Board of Directors, plans for future needs of the system, and the replacement of components. Advises the IT Department on any needs for network maintenance or similar needs. Provides second level of response if any incidents or issues occur.

4.1.3 System Administrator- Provides technical guidance concerning hardware, software, licensing, and evaluates evolving technologies and tools. Administers firewall protection and overall network security measures. Provides third and top level of response if any incidents or issues occur.
4.1.4 IT Department - Provides system access to Local Users and manages provides the day to day management on the local machines and devices belonging to LOWA. Assists the needs of the Local Users and advises Managers of any purchases that may be needed. First level of response if any incidents or issues occur.

4.1.5 Operating Center Managers and Foremen - Work with the General Manager and IT Staff to ensure that adequate tools resources are available to users.

4.1.6 Local Users - Ordinarily access the network for business purposes. Abide by user security requirements set forth by the Board and General Manager, properly use computer equipment, and protect association information. Save their files to the server while using LOWA machines. Are instructed to use best judgment is computer safety and to inquire with the IT Department should any questions arise.

4.2 Operators
4.2.1 Administrators - Have full server access, network rights, and can make decisions based on network direction and implementation. Also manage network function and settings. Primary source for solutions.

4.2.2 Super Users - Have more ability than "users" or "terminal users". Thought of as key staff and managers. Likely to purchase equipment as needed.

4.2.3 Users - Majority unit that has the highest impact on the network. Activity can regulate the direction taken for improvement and network development.

4.2.4 Terminal Users - Lowest impact users, generally only use point of sale devices.

4.3 Equipment
4.3.1 Servers - Dedicated technologies to run network wide processes and functions. High importance. Maintained by Administrators.

4.3.2 Desktops - Most Widespread units. Serve a variety of purposes and are accessed by every user.

4.3.3 Mobile Devices - Includes tablets, smart phones, and laptops. These items are to be safeguarded at all times due to higher risk of data loss.

4.3.4 Other IT Equipment - Technical gear such as routers, switches, cabling, and other miscellaneous objects. These are distributed and administered by the system administrators.

5.0 Exclusions

None. All users are responsible for computer security.

6.0 Procedures

6.1 Enforcement
6.1.1 LOWA's technology may be monitored at all times by the IT Department and its associates. User accounts are accepted upon account setup. Per request, an account can be monitored and reviewed. Pending results of the review, appropriate action may be taken.

6.2 Emergency Action Plan
6.2.1 Anyone discovering a breach or technical issue will immediately contact the IT Department and Senior Management who will notify the Systems Administrator for immediate investigation and resolution. Such action includes alerting the appropriate LOWA personal including the General Manager, the Board if appropriate, local, and federal authorities. A detailed investigation of activities on the network and review of user accounts will be undertaken as deemed appropriate.
7.0 General Rules

7.1 Acceptable Device Use Policy
7.1.1 For all devices the following is accepted upon access: “The device you are activating is the property of the Lake of the Woods Association. Association policy permits your use of this device for business purposes, and tolerates limited, incidental personal use. To enforce this policy and to avoid abuse of the privilege of using this device, the Lake of the Woods Association monitors the use of this device electronically. Any misuse of this device or abuse of this privilege may result in severe consequences, up to and including termination of employment. Please consider this warning carefully before you proceed with any use of this device.” Any necessary software must be installed and updated by the system administrator, unauthorized software will be removed.

7.2 Passwords
7.2.1 Passwords are regulated to be changed every 90 days. Each password must:
- be 8 characters in length
- use upper case letters (A-Z)
- use lower case letters (a-z)
- alphanumeric characters (0-9)
- and non-alphanumeric characters (punctuation symbols)

7.2.2 Passwords may not be repeated when changed. Under limited circumstances a user may share passwords and such instances must be approved by the System Administrator and GM. If available, additional safeguards should be employed.

7.3 Data Use
7.3.1 All data created on LOWA devices is property of the Lake of the Woods Association. All files should be saved onto the appropriate server drive and not on a user’s desktop.

7.4 Email
7.4.1 Association email is to be used for association use and may be used for limited personal use. It is prohibited for users to use the email service for personal internet accounts, newsletters, or other non-work related use. All email communication should contain the disclaimer “The information contained in this message may be privileged and thus protected from disclosure. If the reader of this message is not the intended recipient, or an employee or agent responsible for delivering this message to the intended recipient you are hereby notified that any dissemination, distribution, or copying of this communication is strictly prohibited.”

7.5 Internet Access
7.5.1 Internet access is available on most machines. It is generally used for research and light personal use. Shopping, unauthorized social networking, and other bandwidth heavy uses are prohibited.

7.6 Wireless and Remote Access
7.6.1 Wireless access is open for public use at the buildings where it is available and must be separate from the network.

7.6.2 Remote access or external access to the network is available on an as needed basis and is primarily available to administrators and super users. Standard use rules apply. This should be done through an approved method such as LogMeIn over a secure connection.

7.7 Process Review
7.7.1 This document should be reviewed for effectiveness every 6-9 months and thoroughly reviewed every 2 years.
Effective Date: July 18, 2012

Lake of the Woods Association, INC.

By: Pat Rowland, President

ATTEST:

I, as Secretary for Lake of the Woods Association, Inc., hereby attest that the foregoing Administrative Resolution No.2012-11 was adopted by the Board of Directors at a duly held and noticed Board of Directors meeting held on the 18 day of July, 2012.

Jon Anderson, Secretary