**Statement of Privacy** for Web Based Data Collection & Management

**Privacy Statement**

The Lakeland Area Chamber of Commerce is committed to protecting your privacy and developing technology that gives you the most powerful and safe online experience. This Statement of Privacy applies to the Lakeland Area Chamber of Commerce website located at LakelandChamber.com and all of its sub-domains and governs data collection and usage. By using the Lakeland Area Chamber of Commerce website, you consent to the data practices described in this statement.

**What information do we collect?**

The Lakeland Area Chamber of Commerce collects information from you when you register on our site, place an order, subscribe to our newsletter, respond to a survey, fill out a form or apply to become a member or update your member information.

When ordering or registering on our site, as appropriate, you may be asked to enter your: name, email address, mailing address, phone number, credit card information or other relevant information. You may, however, visit our site anonymously.

The Lakeland Area Chamber of Commerce also collects anonymous demographic information, which is not unique to you, such as information about your computer hardware and software. This information can include: your IP address, browser type, domain names, access times and referring website addresses. This information is used by the Lakeland Area Chamber of Commerce for the operation of the service, to maintain quality of the service, and to provide general statistics regarding use of the Lakeland Area of Chamber of Commerce website.

*Please keep in mind that if you directly disclose personally identifiable information or personally sensitive data through Lakeland Area Chamber of Commerce public message boards or blogs, this information may be collected and used by others.* ***Note: The Lakeland Area Chamber of Commerce does not read any of your private online communications.***

The Lakeland Area Chamber of Commerce encourages you to review the privacy statements of websites you choose to click to from LakelandChamber.com so that you can understand how those websites collect, use and share your information. The Lakeland Area Chamber of Commerce is not responsible for the privacy statements or other content on websites outside of The Lakeland Area Chamber of Commerce.

**How do we use your personal information?**

The Lakeland Area Chamber of Commerce collects and uses your personal information to operate Lakeland Area Chamber of Commerce websites and deliver the services you have requested. The Lakeland Area Chamber of Commerce also uses your personally identifiable information to inform you of other products or services available from The Lakeland Area Chamber of Commerce and its affiliates. The Lakeland Area Chamber of Commerce may also contact you via surveys to conduct research about your opinion of current services or of potential new services that may be offered.

The Lakeland Area Chamber of Commerce keeps track of the websites and pages our customers visit within the Lakeland Area Chamber of Commerce, in order to determine what services are the most popular. This data is used to deliver customized content and advertising within The Lakeland Area Chamber of Commerce to customers whose behavior indicates that they are interested in a particular subject area.

Any of the information we collect from you may be used in one of the following ways:

1. To personalize your experience (your information helps us to better respond to your individual needs)
2. To improve our website (we continually strive to improve our website offerings based on the information and feedback we receive from you)
3. To improve customer service (your information helps us to more effectively respond to your customer service requests and support needs)
4. To process transactions

**Do we disclose any information to third parties?**

The Lakeland Area Chamber of Commerce may, from time to time, contact you on behalf of external business partners about a particular offering that may be of interest to you. In addition, The Lakeland Area Chamber of Commerce may share data with trusted partners to help us perform statistical analysis, send you email or postal mail, provide customer support or arrange for deliveries. Your information may be provided to third party contractors, however, all such third parties are prohibited from using your personal information except to provide these services to the Lakeland Area Chamber of Commerce, and they are required to maintain the confidentiality of your information.

The email address you provide for order processing, may be used to send you information and updates pertaining to your order, in addition to receiving occasional company news, updates, related product or service information, etc.

The Lakeland Area Chamber of Commerce does not use or disclose sensitive personal information, such as race, religion, or political affiliations, without your explicit consent.

The Lakeland Area Chamber of Commerce websites will disclose your personal information, without notice, only if required to do so by law or in the good faith belief that such action is necessary to: (a) conform to the edicts of the law or comply with legal process served on the Lakeland Area Chamber of Commerce or the site; (b) protect and defend the rights or property of the Lakeland Area of Chamber of Commerce; and, (c) act under exigent circumstances to protect the personal safety of users of the Lakeland Chamber of Commerce or the public.

**Does the Chamber’s website use cookies?**

The Lakeland Area Chamber of Commerce website uses “cookies” to help you personalize your online experience. A cookie is a text file that is placed on your hard disk by a Web page. Cookies cannot be used to run programs or deliver viruses to your computer. Cookies are uniquely assigned to you, and can only be read by a Web server in the domain that issued the cookies to you.

One of the primary purposes of cookies is to provide a convenience feature to save time. A cookie can tell the Web server that you have returned to a specific page. For example, if you personalize Lakeland Area Chamber of Commerce pages, or register with the Lakeland Area Chamber of Commerce site or services, a cookie helps the Lakeland Area Chamber of Commerce to recall your specific information on subsequent visits. This simplifies the process of recording your personal information, such as billing addresses, shipping addresses and so on. When you return to the same Lakeland Area Chamber of Commerce website, the information you previously provided can be retrieved, so you can easily use the Lakeland Area Chamber of Commerce features that you customized.

If you prefer, you can choose to have your computer warn you each time a cookie is being sent, or you can choose to turn off all cookies via your browser settings. Like most websites, if you turn your cookies off, some of our services may not function properly. However, you can still place orders over the telephone.

**How do we protect your information?**

The Lakeland Area Chamber of Commerce secures your personal information from unauthorized access, use or disclosure. All supplied sensitive/credit information is transmitted via Secure Socket Layer (SSL) technology and then encrypted into our payment gateway providers database only to be accessible by those authorized with special access rights to such systems, and are required to keep the information confidential.

After a transaction, your private information (credit cards, social security numbers, financials, etc.) will not be stored on our servers. All credit card information is processed according to the Credit Card Association rules and the Payment Card Industry Data Security Standards.

**Changes to this Statement**

The Lakeland Area Chamber of Commerce will occasionally update this Statement of Privacy to reflect company and customer feedback. The Lakeland Area Chamber of Commerce encourages you to periodically review this Statement to be informed of how the Lakeland Area Chamber of Commerce is protecting your information.

This statement was last modified on 12/1/2013.

**Contact Information**

The Lakeland Area Chamber of Commerce welcomes your comments regarding this Statement of Privacy.

LakelandChamber.com

PO Box 3607

Lakeland, FL 33802

(863) 688-8551

**Statement of Security** for Chamber Data

All Chamber employees should review this policy regarding security of information. All staff are responsible to ensure that Chamber data is kept secure according to the policies referenced below.

**Best practices for information security**

* Best practices apply to both electronic and paper records.
* Restricted/confidential information must be stored on Chamber owned network servers that are backed up regularly.
* All Chamber, partner and personally-owned computers, which connect to the Chamber’s network, must have anti-virus software where definition files are current and routinely updated in order to prevent damage or compromise to applications, data, files, and/or hardware.
* The Chamber’s Exchange server is the required secure means for conducting Chamber business. Neither Exchange, nor any other email system, should be used for document retention/storage.
* Use caution when opening email attachments for file types such as .ZIP or .EXE which are known to load malicious software that could compromise your system and data.
* NEVER give your network login password combination to anyone.
* NEVER accept someone else’s login/password combination. Knowing someone else’s password may make you a person of interest in the event of a security incident.
* Do not use the same password for all systems, especially for encrypted files. The Chamber’s password guidelines provide details on how to establish strong passwords.
* Delete old data, especially information that includes social security numbers. Paper copies should be shredded.
* Delete "temporary" files on your computer. These include file attachments opened in email and download files. If these files contain restricted/confidential information, they should be immediately removed or encrypted.
* Keep personal data separate from Chamber data. Follow the same encryption standards for personal data.

**Password Policy**

Lakeland Area Chamber of Commerce significantly relies on the use of Chamber provided credentials (network login and password) to provide access authentication to online information technology resources such as email, institutional data, cloud computing processes and other sensitive services. In particular, passwords are the user’s 'keys' to gain access to Chamber information and information systems. A compromise of these authentication credentials directly impacts the confidentiality, integrity, and availability of IT systems, and Chamber as well as user information. This policy establishes minimum standards for the creation and protection of each person’s Chamber password(s). All users accessing Chamber resources are bound by the requirements as described in this policy, to create and secure their password(s).

**Scope**

This policy applies to all Chamber IT systems and resources that require password authentication. All system administrators and users of Chamber IT resources are responsible for implementing and maintaining the requirements outlined in this document.

Do not use the same password for Chamber accounts as for other non-Chamber access, such as, online banking, personal ISP accounts, Facebook, LinkedIn, Twitter or other social network accounts. This policy does not apply to password-protected files, encryption key passphrases, or local accounts that do not interface with Chamber user account authentication systems.

**Password Requirements**

Individuals must have a unique identifier and password for each Chamber account.

* All Chamber owned electronic devices that access confidential/restricted Chamber data must have password protection enabled.
* Passwords must be stored in irreversible encryption format whenever possible.
* Passwords must contain at least eight (8) characters, in combination as follows:
	+ At least one upper case alphabetic character.
	+ At least one lower case alphabetic character.
	+ At least one numeric character (1, 2, 3, etc.).
	+ At least one punctuation or symbol character (@, $, #, etc.).
* Do not use ‘ “ or blank spaces as they may not work with all systems.
* Passwords must be changed at least once every six months.

**Selecting a password you can remember**

Long, cryptic passwords are the most secure but can be difficult to remember. One method of selecting a good password is to start with a short sentence, for example, a holiday greeting: Merry Christmas and Happy New Year

By using the first letter of each word it becomes MCaHnY. It has a mixture of upper and lower case letters and some characters are typed with the left hand and some with the right. It is only six characters long so it needs to have at least two more characters, either numeric digits or punctuation. Here are three possibilities:

* 1MCaHNY!
* Mcahny!!
* MCaHnY2y

**Passwords should not be**

* Names of family, pets, friends, co-workers, fantasy characters, etc.
* A word in any language, slang, dialect, jargon, etc.
* Computer terms and names, commands, sites, companies, hardware, software, etc.
* Personal information such as birthdays, addresses, phone numbers, etc.
* Words or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
* Any of the above spelled backwards.
* Any of the above preceded or followed by a digit (e.g. secret1, 1secret).

**Password don’ts**

* Don't reveal passwords over the phone to anyone.
* Don't reveal passwords in an email message.
* Don't talk about passwords in front of others.
* Don't reveal passwords on questionnaires or security forms.
* Don't share passwords with anyone, including family members.
* Don't reveal passwords to co-workers while on vacation or leave.
* Don’t use the "remember password" feature of applications.
* Don’t write passwords down and store them anywhere in your office.
* Don’t store passwords in a file on any computer system including smart phones, PDAs, or similar devices, unless that file is encrypted.
* Don’t use the same password for Chamber accounts as for other non-Chamber access.
* If someone asks for your password, refer them to this document.

**Using Mobile Devices to Store or Access Chamber Information**

This policy is necessary to protect the confidentiality, availability, and integrity of Lakeland Area Chamber of Commerce and Chamber affiliates’ information while stored, transmitted or processed on mobile devices.

**Scope**

It applies to any mobile device that is used to store or access Chamber information.

**Policy**

Any mobile device accessing or storing Chamber restricted/confidential or internal information is subject to all University policies and in addition, will adhere to the following.

If the capability exists for the device, mobile devices will be configured to:

* Receive and install security updates from the operating system vendor.
* Have anti-virus software enabled, active, and up to date.
* Use a device and/or screen saver password. Portable computing devices must, at a minimum, be password protected in accordance with Chamber policy.
* Have an operating system-level firewall installed and active with exceptions being approved by the Chamber’s managed network service provider.
* Connect to restricted/confidential or internal data using the security protocols required by the managed network service provider. This may include secured connections and use of the Virtual Private Network (VPN) software.
* Have physical security measures in place when not in use. This means the device must be secured, e.g. locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet with a cable lock system.

The Chamber, at their discretion, may restrict the access of any mobile computing device to Chamber data if the mobile computing device presents a threat to the integrity of data or other computing resources.

**Definitions**

A **mobile device** is any type of device that is designed to be moved and is capable of collecting, storing, transmitting, or processing electronic data or images. Movement in this case refers to the device generally not having a fixed connection to the network. Examples of mobile computing devices include but are not limited to a laptop or tablet PC, Smartphone, or a USB flash drive.

**Justification**

Mobile devices are very popular because of their convenience and portability. The use of such devices, however, is accompanied by risks that must be recognized and addressed to protect both the physical

devices and the information they contain. The most effective way to secure confidential data is not to store it on mobile devices. This can be accomplished by storing sensitive data only on secure central Chamber servers and accessing it remotely using secure communication technologies. It is the responsibility of the user to recognize these risks and take the necessary steps to protect and secure their mobile device.

**What happens if data are lost**

Notify the local police if a device is missing or stolen. Notify managed network service provider at support@boring.com. If it is a personally-owned device that contains University data follow these same procedures.

Having your data encrypted means if your device is lost, the data are not lost.