# Survey Confidentiality

ModernThink is committed to ensuring the methodology and integrity of our surveys and research are able to withstand the strictest scrutiny. As part of that commitment, we take multiple precautions to protect the confidentiality of survey takers' responses. Examples of efforts to ensure confidentiality include, but are not limited to, the following:

- Usernames and passwords are randomly generated, so they cannot be accidentally accessed by unauthorized participants. No participant will be able to access another participant's data, since entry is username/password protected and survey identifiers are unique.
- All survey takers are provided with a confidential, toll-free Help Desk, which they can call anonymously with any questions or concerns.
- We only report data back when there are five or more respondents in a particular demographic category.
- Questions about demographics are strictly on an optional basis, unless otherwise disclosed to the survey takers.
- Participants are advised that association leaders and/or the survey committee will be given verbatim transcripts of the responses to the open-ended questions. Anyone wishing to maintain his/her anonymity should refrain from using his/her name and/or any other identifying characteristics in those open-ended remarks.
- ModernThink collects and stores all of the data on its secure servers directly under our control.
- ModernThink provides a secure connection for online survey participants. The web server employs an SSL certificate for securing the survey web site. This provides SSL encryption with identity authentication and guarantees every SSL session receives 256-bit SSL encryption, regardless of browser version.
- The database servers are backed up on a daily basis with backups stored at designated, secure offsite locations. Bandwidth to servers is redundant and expandable to handle high-traffic surges.
- Because the survey data and other research information are added to our benchmarking and best practices database, it is retained indefinitely.
- Within one year after the survey closes, any identifying account information is expunged.

In the event of a security breach, ModernThink has processes in place to take any breached system off-line or lock all network ports until all issues are remedied. ModernThink servers have notifications in place to alert all administrators in case any user logs into the server for any purpose. The notification describes which user logged in and from which address. In the event of loss, release or unauthorized access of client data, it is our expressed policy to notify all parties involved to jointly identify the appropriate service recovery plan. On the chance that a breach occurs, affected clients would be notified within 24 hours of the detection of the breach. ModernThink has never experienced any significant data integrity issues that might potentially compromise client data.