

radio2dot0, Ltd. Statement of Privacy Procedures

Last revised June 13, 2009

Section 1: Information Collected about you

When you visit our website: each visit to the public sites maintained by us (www.radio2dot0.com, www.virtualnewscenter.com, and www.advantageweather.net) is logged in two ways. First, the web server logs each item served – text, image or other file – recording the IP address, date of access, and information provided by your browser such as the operating system and browser software version numbers. Second, code within the HTML separately records the same information and makes it available to us via StatCounter.com and Google Analytics. We use this information in aggregate only, to establish the marketing effectiveness of our various pages. The same information is collected concerning visitors to any blog we maintain on your behalf.

When you click a link in an email solicitation from us: In addition to the logging above, the URLs contained in our email links include an ID number that we use to aggregate your visits to our site over time. We make no other use of this information than to respond to your action by telephone.

When you send us email: we utilize Google Mail to host our email. Their use of the data collected is governed by their privacy policy. We routinely maintain within the Gmail-hosted system all emails we send/receive unless they are news releases or otherwise pertain directly to the information we air within your newscasts. Those emails are deleted once they are no longer timely. We do not attach any tracking ID to links in our customer e-mail; only initial solicitations are ID'd as described above.

Customer records: We maintain a single printed copy of the contract you originally signed for our service, and a digital copy is maintained in PDF form. We maintain your billing information, payment history and outstanding balance information in Intuit's QuickBooks software, accessible by only one staff member.

Section 2: How We Secure Your Information

Website visits: all information maintained by StatCounter and Google Analytics is accessible only through https URLs and we maintain no physical record of it. StatCounter deletes visit records on a rotating basis, and only the 500 most-recent visits are available at any level of detail. Google Analytics' data retention is a matter covered by their privacy policy. Our web server deletes archived visit logs after 4 weeks, and no backups of the log files are kept.

Email: All email access is through https URLs, and all our staff members maintain secure passwords as required by Google. Google maintains backups and archives of all email handled by their system. Retention and destruction is a matter covered by their privacy policy. We do not separately maintain email in any way.

Customer Records, Payments: Your payments are processed by only one member of our staff. They are recorded in the software and deposited in the bank the same day they are received, and no physical

copies are retained. Our bank, Commerce Bank, conforms to the current Check 21 procedures and requirements for check handling. If your check includes a stub or remittance advice, that information is shredded. Access to QuickBooks is limited to one person, who must choose a new high-security password every 90 days. The software is installed on only one computer and the data file is stored on a hard drive under 256-bit encryption. The computer is not accessible remotely. Our digital copy of your contract is maintained on the same secured hard drive. The encrypted file is routinely backed up to a secure off-site storage area. In addition to the security provided in the online backup process, the encrypted data is stored as a single file, and individual records cannot be access without mounting and decrypting the entire file, which is protected by a high-security password. Our printed copy of your contract is maintained without any extraordinary security procedures, as this is the same document required by the FCC to be placed in your station's public file.

Physical Security: our publicly-accessible web server is maintained in a secure data center in Cleveland, OH, accessible only after identity verification by multiple means. Remote access to the server is accomplished only through secure protocols and never on publicly-shared Internet connections (such as in hotels). Complex passwords and multiple levels of authentication are used for all remote access. Our billing computer and files are maintained in a home office and physical security is as one would expect in a home environment. We run antivirus, spyware- and rootkit-detection, and firewall software and hardware on all computing systems having contact with customer data.

Section 3: Information Retention and Destruction

Website & Email: Covered in Section 2 above.

Customer Records: we maintain the described records for the duration of your relationship with us. At some future time, we anticipate the need to archive data once it reaches 3 years of age, for reasons of storage space. We will maintain the same security over archived data that we do over live data. We anticipate retaining digital and paper copies of contracts permanently.