Privacy Statement

Poison Help Campaign General Population Survey

OMB Control No. 0915-0343

KRC RESEARCH ASSURANCE OF PRIVACY OF SURVEY DATA

KRC Research understands the importance of confidentiality and privacy. KRC routinely partners with clients with heightened security requirements, such as governments, healthcare companies, and financial services organizations.

Procedures for Maintaining Privacy

1. We carefully observe all non-disclosure agreements. Even in the absence of explicit non-disclosure contracts, we never share client documents or research results without client permission. This is at the core of KRC's employee Code of Conduct, which all employees sign annually and which is the subject of annual online training;
2. We guarantee the confidentiality and anonymity of our research respondents (consistent with research industry codes of conduct). For example, access to data files used for sampling is generally limited to supervisors, and individual-level personally identifiable information is removed from files before they are transmitted;
3. KRC's data security protocols include storing electronic materials in password protected files on KRC servers, utilizing secure file transfer, secure data repositories, ensuring third-party data processors are bound by appropriate confidentiality obligations and procedures, and removing personally identifiable information from data files upon completion of projects; and
4. Rigorous procedures and policies are in place throughout our organization to ensure systems are up-to-date and secure. Below is a snapshot of our technology security policies and procedures:
    - All PCs and servers have centrally managed, enterprise level anti-virus software running at all times;
    - All incoming e-mail messages and attachments are scanned for viruses;
    - Anti-virus scans of all files on local drives are performed daily;
    - Anti-spyware is installed on all PCs and workstations and hard drives are scanned daily for anti-spyware software;

- All access points to our network are approved and have an associated risk assessment;
- All external access to our company network is controlled through a firewall which among other purposes denies all inbound and outbound traffic without business purposes;
- Cryptographic standards are in place for the protection of information;
- All workstations and laptops are encrypted with AES 256-bit level whole disk encryption;
- Intrusion detection technology is used at the network level;
- A documented information systems business continuity and disaster recovery plan is in place;
- Individual accounts are established for each employee that are password protected;
- Passwords are changed at least every 60 days and have multiple levels of complexity; and
- All policies are consistent with government laws, regulations, and directives.

Our vendors also have firewalls and these kinds of IT security policies, and we are always happy to reconfirm these policies in advance of any project.