Adoption and Implementation of a Privacy Policy
An organization engaged in online activities or electronic commerce has a responsibility to adopt and implement a policy for protecting the privacy of individually identifiable information. Organizations should also take steps that foster the adoption and implementation of effective online privacy policies by the organizations with which they interact; e.g., by sharing best practices with business partners.

Data Security
Organizations creating, maintaining, using or disseminating individually identifiable information should take appropriate measures to assure its reliability and should take reasonable precautions to protect it from loss, misuse or alteration. They should take reasonable steps to assure that third parties to which they transfer such information are aware of these security practices, and that the third parties also take reasonable precautions to protect any transferred information.

Data Quality and Access
Organizations creating, maintaining, using or disseminating individually identifiable information should take reasonable steps to assure that the data are accurate, complete and timely for the purposes for which they are to be used. Organizations should establish appropriate processes or mechanisms so that inaccuracies in material individually identifiable information, such as account or contact information, may be corrected. These processes and mechanisms should be simple and easy to use, and provide assurance that inaccuracies have been corrected. Other procedures to assure data quality may include use of reliable sources and collection methods, reasonable and appropriate consumer access and correction, and protections against accidental or unauthorized alteration.

Notice and Disclosure
An organization’s privacy policy must be easy to find, read and understand. The policy must be available prior to or at the time that individually identifiable information is collected or requested. The policy must state clearly: what information is being collected; the use of that information; possible third party distribution of that information; the choices available to an individual regarding collection, use and distribution of the collected information; a statement of the organization’s commitment to data security; and what steps the organization takes to ensure data quality and access. The policy should disclose the consequences, if any, of an individual’s refusal to provide information. The policy should also include a clear statement of what accountability mechanism the organization uses, including how to contact the organization.

Choice/Consent
Individuals must be given the opportunity to exercise choice regarding how individually identifiable information collected from them online may be used when such use is unrelated to the purpose for which the information was collected. At a minimum, individuals should be given the opportunity to opt out of such use.
E-commerce has grown faster than anyone could have predicted only a few years ago. The Internet is entering more and more American homes to become a true mass medium. While the Net offers unparalleled convenience for consumers, many hesitate to transact business on the web. People are nervous about the potential loss of personal privacy. Is their personal information and online activity tracked, collected and analyzed without their knowledge or approval?

Web businesses are striving to convert visitors to customers. But consumers will not purchase from sites if they do not feel confident that their personal information is respected. News stories, studies and polls all confirm that fear of the loss of privacy is a principal reason people don’t transact business online. If online companies expect consumers to spend time at a Web site, make purchases and visit the site again they must build trust.

Posting a privacy policy is a critical step. But what is a credible privacy policy? The Online Privacy Alliance, a coalition of nearly 100 global companies and associations, urges all Web businesses to post privacy policies that contain ALL the following elements, recognized by policymakers and consumers as the foundation for a policy that engenders trust.

Organizations collecting personal data are urged to join an online privacy “seal program.” Information on these programs is available at the following Web sites:

- www.bbbonline.org
- www.truste.org
- www.cpawebtrust.org

Other third party enforcement programs are at:

- www.the-dma.org
- www.irsg.org

Thanks to Intel Corporation for their support in the creation of this brochure.

Join Us! To join the Online Privacy Alliance, or for more information, contact: www.privacyalliance.org
Or contact 202/244-1200.