

Network Protection for Design Professionals

Privacy Policy

Background:

Privacy policies are needed for any organization handling Nonpublic Personal Information (NPI). Depending on your organization's operations and the type of information handled, specific regulatory guidelines may apply to the implementation and content of such a policy. Some examples include:

- The Gramm-Leach-Bliley Act (GLBA) — addresses consumer financial privacy
- Health Insurance Portability and Accountability Act (HIPAA) — addresses the privacy of personal health care information
- Children's Online Privacy Protection Act (COPPA) — applies to the on-line collection of information from persons under 13 years of age

In general, a privacy policy details what information you gather from the persons or entities that you do business with, how it is protected and the situations in which this information may be shared with a third party.

How to implement appropriate controls:

Implement, prominently disclose and honor a privacy policy following the general guidelines provided below. Note that the guidelines provided are derived from Federal Trade Commission information on compliance with GLBA. GLBA is one of the most widely applicable privacy regulations but may or may not apply to your organization's operations. Consult your attorney when drafting the specific language of your privacy policy.

- Design your policy with your customers in mind. Your privacy policy should be clear, direct and easy to understand.
- Say what you mean and mean what you say. The FTC has taken privacy actions against companies that overstated their security measures and experienced a security breach which contradicts the standard of care portrayed in the policy. Treat these statements the same as advertising claims you make.
- Call customer attention to any changes in policy. If you modify how you gather or use personal information you must call the customers attention to the change in policy.
- Create a culture of compliance. Train all employees on the organization's privacy policy and how to protect sensitive data.

Resources:

Privacy Policies: Say What You Mean and Mean What You Say, Federal Trade Commission,
<http://www.ftc.gov/bcp/edu/pubs/articles/art09.shtm>

GETTING NOTICED: Writing Effective Financial Privacy Notices, Federal Trade Commission,
<http://www.ftc.gov/bcp/online/pubs/buspubs/getnoticed.shtm>

In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act, Federal Trade Commission
<http://www.ftc.gov/bcp/online/pubs/buspubs/glbshort.shtm>

