The Privacy Policy Problem (1):
A Model Policy

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Many organizations strive to protect the confidentiality of prospects and clients. In this column and the next three, I want to explore issues relating to privacy policies and the sometimes problematic relations between legitimate, well-meaning institutions and the commercial organizations with which they do business – and the criminal organizations which abuse their good names and reputations.

Norwich University’s Privacy Policy<http://www.graduate.norwich.edu/privacy_policy.php> stands as an excellent example of a clear, well-written and comprehensive document – an example that could usefully be considered by readers of this column who may need a sample policy for their own organization’s use. Links to the policy are available where visitors may enter personally identifiable information (PII); for example, the admissions-related pages have links at the bottom of every page with a data-entry form. Specifically, the policy makes the following essential points (quoting with added commentary in square brackets):

- “Norwich University requests a certain amount of information from our clients in order to provide the online experience.” [A privacy policy should begin with a statement of the purpose of data collection.]
- “Although we gather names, e-mail addresses, locations and other personal information (dependent on the platform being used), all information is kept confidential.” [The introduction makes the intent of the policy clear.]
- “Information is used for course registration, billing purposes, providing knowledge about our client base, managing our services and to assist us in making the online experience the best possible.” [These are useful clarifications of the intended applications for the collected data.]
- “Information about who may login in from time to time is analyzed in order to allow us to monitor and maintain our network. Information about our clients may also be used to provide feedback to our institutional clients; at no time do we share this information with an outside source. We may, from time to time, examine a platform for statistical purposes, but we will not identify any individual in doing so.” [These are specific constraints on how the data are to be used.]
- “Information placed on our systems may be available to others on our various platforms, depending on the platform chosen. This information is used strictly to allow a client to participate in their individual course(s) and is kept confidential. We will not divulge private information to any unauthorized person.” [These sentences add some more well-defined constraints.]
- “It is understood that information entered on our system(s) may be seen by a variety of people administering, participating in or monitoring any part of the chosen platform, within the reasonable guidelines set therein.” [Although this alert may seem obvious to information technology specialists, it is worth reminding non-technical people of the reality of data collection.]
- “[Norwich] will also comply with any legal request(s) made by any body so authorized
for information, should proper documentation be provided to us.” [This is the get-out-of-jail card that puts users on notice that the University will fully comply with all appropriate court orders and other legal obligations from duly constituted authorities.]

In my next column, I’ll look at the problems which can occur when working with independent partner organizations that may have different privacy policies from one’s own.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.graduate.norwich.edu/infoassurance/> and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2008 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.