PREVALENT networks

Writing Effective Policies

Using Written Policy to Manage Behavior, Mitigate Risks, & Maximize Compliance

Written By: Nancy Flynn
The ePolicy Institute

The ePolicy INSTITUTE™
www.ePolicyInstitute.com

Founder & Executive Director, The ePolicy Institute
Author, Handbook of Social Media (2011), The ePolicy Toolkit (2011), The e-Policy Handbook, E-Mail Rules, Instant Messaging Rules, Blog Rules, Writing Effective E-Mail, E-Mail Management, and other books

Overview

Prevalent Networks, www.prevalent.net and The ePolicy Institute™, www.epolicyinstitute.com, have created **Writing Effective Policies: *Using Written Policy to Manage Behavior, Mitigate Risks & Maximize Compliance***, a best practices-based business guide for human resource professionals, legal and compliance officers, training managers, IT decision-makers, information security managers, business owners, and anyone who plays a role in writing, implementing, and managing workplace policies.

Through the implementation of a strategic policy management program, incorporating clear and comprehensive written policies, formal employee education, and a proven-effective policy management solution, organizations successfully can manage their legal, regulatory, and organizational risks and compliance obligations.

Writing Effective Policies: *Using Written Policy to Manage Behavior, Mitigate Risks & Maximize Compliance* is produced as a general best-practices guide with the understanding that neither the author, ePolicy Institute Founder & Executive Director Nancy Flynn, nor the publisher, Prevalent, is engaged in rendering advice on legal, regulatory, or other issues. Before acting on any policy or procedure addressed in this whitepaper**,** you should consult with legal counsel or other professionals competent to review the relevant issue.

Introduction:

Why Every Organization Needs Effective Written Policies

Regardless of whether your enterprise is public or private, large or small, for-profit or not-for-profit, regulated or unregulated, all organizations need effectively written and strategically managed business policies.

- Effective written policies communicate organizational, legal, and regulatory rules to full- and part- time employees, executives and board members, independent contractors and consultants, and others working on behalf of your organization.

- Effective written policies provide employees with a clear understanding of what constitutes appropriate, acceptable, and lawful business behavior.

- Effective written policies help employers demonstrate to courts and regulators, employees and applicants, customers and investors, the media and decision-makers, and other important audiences that the organization is committed to operating a business environment that is civil, compliant, and correct.

Through the strategic implementation of a business policy program that combines written rules with employee education supported by policy management tools, employers in all industries and professions can minimize (and in some cases prevent) potentially costly and protracted risks, while mandating appropriate business behavior, and maximizing compliance with legal, regulatory, and organizational guidelines.

Three-Step Formula for Policy-Writing Success

Regardless of your comfort, skill, or experience as a business writer, you can improve the quality of your policy writing, enhance the effectiveness of your written rules, and magnify the success of your compliance management program simply by applying this three-step formula for policy-writing success:

Step 1.	**Pre-Writing:**	Conduct a policy audit.
Step 2.	**Writing:**	Create well-written policies.
Step 3.	**Post-Writing:**	Manage policy compliance.

I. PRE-WRITING BEST PRACTICE: CONDUCT A POLICY AUDIT

Before you start writing or revising policies, first take a clear-eyed look at your current business policies from a legal, regulatory, and organizational standpoint. In other words, conduct a formal audit of your existing policy program.

Understandably, you will need to create separate audit questionnaires and undertake separate audits for nearly every business policy you plan to write or revise. After all, the legal, regulatory, and organizational risks and rules that should be addressed in an email policy are entirely different from those of a corporate vacation policy. Best practices call for: (A) One free-standing audit per policy; and (B) One stand-alone policy per technology (email), situation (vacation), or behavior (harassment & discrimination) that you seek to manage through formal rules.

While the nature of your policies will determine the exact content of your audit questionnaires, in general you'll want to uncover the following types of information in the course of a workplace policy audit:

1. Policy audience and goals: Who is the intended audience for this policy? Why does this particular situation/behavior/technology merit formal rules? What does the organization hope to accomplish with this policy? Is there a proven need for this policy? What benefits will this policy deliver to the organization and its employees? Are employees likely to respond positively or negatively to this policy?

2. Review policy-related legal and regulatory risks and rules. Assign your legal counsel or compliance officer the task of reviewing current federal/state laws and government/industry regulations governing the situation/behavior/technology addressed by the policy in question. Determine exactly what your organization needs to do—from the standpoint of policy, training, and management technology—to achieve legal and regulatory compliance on the federal level and in all states in which you do business, have customers, or litigate lawsuits.

   Laws and regulatory requirements vary by jurisdiction and industry, so it is essential for you to do your homework before writing policy. For example, Social Media Policy, Email Policy, and Text Messaging Policy would all be written in the context of monitoring laws, e-discovery rules, and electronic record retention guidelines set forth by federal and state courts. Similarly, if your company handles private consumer information including Social Security and credit card numbers, then your Confidentiality Policy may need to address Data Breach Notification Law, the Gramm-Leach-Bliley Act, PCI-DSS, and State Encryption Law.

3. Review policy-related organizational risks facing your company and employees. Has excessive absenteeism led to a slide in workplace productivity? Have you been forced to terminate otherwise valuable employees because of inappropriate computer use? Has offensive behavior by managers triggered hostile work environment or harassment claims by staff? Has inconsistent policy enforcement led to resentment among employees? If your focus is on the creation of effective electronic policies, then you'll need to evaluate the ways in which your organization accesses and uses email, the Web, and other electronic business communication tools and technologies. Do you provide employees with Smartphones? Do employees use IM, text messaging, or mobile devices for internal/external communications? Do you retain and archive email and other forms of electronically stored information? Do you allow personal use of the company email system? Are employees allowed to access private email accounts, visit non-business-related Web sites, or post personal Tweets during the workday?

4. In the age of social media, many organizations are adopting policies to manage Facebook, YouTube, Twitter, LinkedIn, and other networking sites. If you're embarking on a Social Media Policy, be sure to research employees' after-hours social media use in the course of your policy audit. Are employees using personal blogs and social networking sites to comment on your business? Do employees go online after hours to whine or complain about their jobs? Have employees accidentally or intentionally leaked confidential business or consumer information that could damage the organization's reputation, trigger a lawsuit, or jumpstart a regulatory investigation?

5. Take a close look at all of your organization's existing business policies. Do you have in place separate policies governing all technologies (email, Internet, text messaging, blogs, mobile devices, etc.), situations (vacation, attendance, dress code, etc.), and behaviors (harassment & discrimination, ethics, code of conduct, etc.)? When is the last time your company updated its policies?

6. Are your current policies well-written? Are they easy to read, understand, and adhere to? Do you have a skilled business writer on staff to write and revise policies, or will you need to retain the services of a freelance policy writer to produce effective policies?

7. Are your policies well-designed and visually appealing? Does the "look" of your policies enhance their readability? Do you employ an in-house designer who is adept at producing readable, visually appealing policies? Or will you need to hire a freelance designer to handle policy design and production?

8. How do you distribute policies to employees? Best practices call for policy distribution in the course of formal employee training. Yet, most employers rely solely on the employee handbook or Intranet to introduce policies to workers,

according to American Management Association/ePolicy Institute research. Policy distribution is critical. There's no point writing policies if no one knows they exist.

9. The results of your policy audit will help you identify and understand the specific risks facing your organization. Based on your audit findings, you are now ready to update old policies and, as necessary, create new policies for 2011.

10. Be sure to date each new and revised policy before putting it into circulation. Collect and destroy all but one file copy of your old policies. Make sure every employee receives or has access to one copy of each new and revised policy.

11. Repeat the policy audit process annually.

II. BEST PRACTICES FOR WRITING EFFECTIVE POLICIES

Use Clear & Specific Language

Whether you are creating policies governing attendance and dress, ethics and conduct, text messaging and mobile devices, or data security and confidentiality, effective written policies should incorporate clear and specific language that is not open to interpretation by individual employees.

Take Email Policy, for example. In Email Policy, it is not enough to say that employees are allowed a "limited amount of appropriate, personal email use." To some employees, "appropriate, personal use" may mean hours spent emailing family and friends. To the CEO, on the other hand, it may mean 15 minutes of "essential" personal communication with family, teachers, babysitters, and physicians before and after regular working hours, during the lunch hour, and in the course of other work breaks.

In the case of email, use written policy to spell out exactly how much personal messaging employees may engage in, with whom, under what circumstances, for how long, and during what periods of the day. Remind employees that, while the policy allows for authorized personal email, those personal messages will be monitored and may be retained along with business-related email. Employees therefore have no reasonable expectation of privacy when using the company system. They should never put in writing any comments that could haunt them, harm the company, or embarrass their family and friends. That is the type of specificity that effective policy writing demands.

Include Content Rules in Polices Governing Communication

Included among the content guidelines that you'll want to incorporate into policies governing any form of communication—electronic or traditional, written or verbal, in-person or via the telephone—are the following rules:

- No violations of regulators' content rules.
- No illegal content.
- No harassment or discrimination based on race, color, religion, sex, sexual orientation, national origin, age, disability, or other status protected by law.
- No disclosure of confidential company, executive, or employee data.
- No exposure of customers' personal financial data to outside parties.
- No disclosure of patients' electronic protected health information to third parties.
- No rumors, gossip, or defamatory comments—about anyone.
- No whining or complaining about the company, customers, or business.
- No external distribution of internal email or other eyes-only data.
- No disclosure of company financials to outside parties.
- No "funny" cartoons, videos, photos, files, or art.
- No obscene, off-color, pornographic, or otherwise inappropriate and offensive language, art, or other content.
- No netiquette (electronic etiquette) breaches.

Use Written Policy to Define Key Concepts and Terms

Don't assume that your employees are familiar with or understand key concepts and terms including, for example, *confidential, intellectual property, trade secret, electronic protected health information, business record, private consumer data*, and the list goes on and on. If you use potentially confusing words or terms in your policy, be sure to provide a definition, either within the text or as part of a glossary of terms at the end of the policy.

Write Policies in Plain English

To help minimize organizational risks and maximize employee compliance with rules, be sure to write policies in plain English. No legal gobbledygook. No confusing technology terms. No acronyms or abbreviations that may not be understood by all employees. Focus on your reader, not yourself. Remember, the purpose of policy is to establish rules and enforce compliance. To that end, policies must communicate with employees—not confuse them.

Adhere to the ABCs of Effective Policy Writing

A is for Accuracy. As a policy writer, your organization relies on you to do your homework vis-à-vis laws and regulations, get your facts straight, and present accurate, reliable, trustworthy information and rules. Accuracy also requires you to adhere to the rules of grammar, punctuation, and style. Compliance management rides on the information you present in written policies, so be sure you *always* get *everything* right.

B is for Brevity. Unless you want employees' eyes to glaze over, do not produce one massive policy document that covers, for example, the use of all electronic business communication tools and technologies (email, IM, text messaging, social media, Web, blogs, software, cell phones, etc.). Increase the odds of having employees read, remember, and adhere to written rules and policies by writing and distributing separate, brief policy documents covering the use of each individual business communication tool. Keep each policy short, simple, and straight to the point. Period.

C is for Clarity. Clarity is essential to communication and compliance success. Your job as a policy writer is to present material in a clear and compelling manner. You must make it easy for employees to read through a policy from beginning to end, then take appropriate action: comply with the rules. You simply cannot expect employees to take time to decipher illogical sentences and paragraphs, struggle through policies that are riddled with grammar goofs and selling errors, or adhere to policies that put them to sleep.

Use Effective Design to Enhance Readability

- Use white space or blank space to enhance policy readability and add visual impact.
- A 10-page, double-spaced policy that is accessible and easy to read is considerably less intimidating than a two-page, single-spaced policy that is crammed full of dense information written in a tiny typeface.
- Rely on boldface headlines and subheads to emphasize important points.
- Communicate rules and other important policy information in small, bit-size chunks. Use bulleted or numbered lists to enhance readability.
- Include a Table of Contents in lengthy policies to help employees locate information quickly when questions or concerns arise.
- Include a glossary of legal, regulatory, technical, business, and other terms to help eliminate confusion, enhance awareness, and support compliance.
- Include contact information for policy team members. Let employees know who to contact when policy-related questions arise.

III. POST-WRITING: BEST PRACTICES TO MANAGE POLICY COMPLIANCE

Support Written Policy with Employee Education

Now that you've completed your policy audit and have written or revised your policies, it's time to educate your workforce about risks, policy, and compliance. Tips for effective policy training:

1. Before distributing policies to employees in the course of training, be sure to have your legal counsel review and sign-off on every policy. The purpose of a legal review is to ensure that your policies address and support compliance with laws (federal and state) and regulations (government and industry) impacting your business. Policy that has been reviewed and approved by legal counsel will help put your organization on firmer legal ground should you one day find yourself battling a workplace lawsuit or facing a regulatory investigation.

2. You cannot expect an untrained workforce to be a compliant workforce. Educate everyone, from entry-level staff to C-level executives, about risks & rules, policies & procedures.

3. Emphasize the fact that policy compliance is 100% mandatory.

4. Approach policy training as an ongoing, continuing education program, not a one-time event.

5. Best practices call for onsite training. Alternatively, you may conduct policy training via live webcast or interactive online training modules.

6. Review policy-related legal, regulatory, security, productivity, public relations, career, and other risks facing individual employees and the organization as a whole.

7. Remind employees that, when it comes to business communication (electronic or traditional, in person, in writing, or over the phone), the easiest way to control risk is to control content. In other words, be mindful of what you say and write.

8. Stress the fact that a policy is a policy. Make sure employees understand that all employment policies apply 24/7/365—at work, home, and on the road.

9. Educate employees about confidentiality, trade secrets, and private information. Explain the legal and regulatory risks facing the company if consumers' private financial data or patients' electronic protected health information is breached, or company financials or other secrets are revealed.

10. Review monitoring and surveillance policies and procedures. Explain the fact that the organization has the legal right to monitor computer activity, videotape employees, and conduct security-related surveillance internally and externally. Explain privacy rights, misperceptions, and the First Amendment.

11. Review sets of related policies. For example, in the course of Email Policy or Social Media Policy training, you would also cover Record Retention Policy, Cell Phone/Mobile Device Policy, Confidentiality Policy, Netiquette Policy, and other relevant policies.

12. Provide every employee with one copy of each written business policy. Make policies available in hard copy during formal training. Make policies accessible at all times to authorized employees via the Prevalent Policy Portal.

13. Do not conclude training until you are certain that every employee understands the policy and is clear on what constitutes policy compliance.

14. Conclude training with a certification quiz, designed to demonstrate to courts, regulators, and management that employees have received (and understood) policy training.

15. Require all employees to sign and date acknowledgement forms attesting that they understand policies and agree to adhere to them, or face the consequences, up to and including termination.

16. Maintain policy and training-related records. Keep copies of policies, training sign-in sheets, certification quizzes, signed acknowledgement forms, training manuals, PPTs, scripts, handouts, etc. In the event of a lawsuit or regulatory investigation, you may need these records to demonstrate that your organization has done its due diligence when it comes to mitigating risks, managing behavior, and enforcing compliance.

Manage Policy Compliance with Prevalent Policy Portal

Once effective policies are written and employee training is complete, best practices call for the effective management of policies and compliance. Prevalent Policy Portal provides a simple, automated solution that enables employers to view policies, search policies, edit polices, certify employee awareness and understanding of policies, and print out policies. Prevalent Policy Portal simplifies policy management and compliance by organizing policies in a central, searchable repository. In addition, Prevalent Policy Portal CCS Connector provides a link to Symantec Control Compliance Suite (CCS)—the market-leading governance, risk, and compliance platform—enabling you to test your policies against IT resources and procedures to determine policy effectiveness, make adjustments as necessary, and maximize legal, regulatory, and organizational compliance. To learn more about Prevalent Policy Portal benefits, visit www.prevalent.net.

Summary:
Apply the Three Es of Policy Compliance Management

Help protect your organization's assets, reputation, and future by adopting a strategic program that incorporates the three Es of policy compliance management:

#1. **Establish** written policies governing every technology, situation, and behavior that you seek to manage through formal rules.

#2. **Educate** all employees about organizational, legal, and regulatory risks and rules, policies and procedures.

#3. **Enforce** written policies with Prevalent Policy Portal, integrated with Symantec Control Compliance Suite (CCS), enabling you to view, implement, aggregate, and manage corporate policies easily and effectively.

About Prevalent Networks

Prevalent Networks is an IT consulting company that works with the leaders in governance, risk, infrastructure, and compliance to deliver solutions that create "information anywhere, security everywhere" (TM). Headquartered in Warren, New Jersey, Prevalent Networks has regional sales offices in: New York City, Boston, Washington DC, Philadelphia and Houston.

Prevalent Networks remains relevant and innovative by creating value by leveraging Prevalent's association with leading technology partners, Prevalent is able to deliver industry leading technology solutions tailored to our clients needs. Prevalent Networks professional services offers consulting engagements let by industry experts with deep knowledge and experience

As clients have demanded different ways to purchase and operationalize technology, Prevalent has developed hosted and managed services that marry leading edge technology hosted in Prevalent's cloud environment and run by our knowledgeable and experienced staff. The result is reduced time to value, reduced infrastructure requirements, and increased security and compliance readiness

In January 2011, CRN named Prevalent one of its 25 national Need to Know Security VARs.

About The ePolicy Institute

The ePolicy Institute is dedicated to helping employers limit email and Web risks, including litigation, through effective policies and training programs. The author of 11 books including the *Handbook of Social Media* (2011), *The ePolicy Toolkit* (2011), and *The e-Policy Handbook*, Founder and Executive Director Nancy Flynn is an in-demand policy writer, trainer, and consultant. She also serves as an expert witness for the federal government and law firms on electronic policies and procedures. Since 2001, ePolicy Institute has collaborated with American Management Association on annual surveys of workplace policies and best practices. A respected media source, Nancy Flynn has been interviewed by thousands of media outlets including *Fortune*, *Time*, *Newsweek*, *Wall Street Journal*, *US News & World Report*, *USA Today*, *New York Times*, NPR, BBC, CBS, CNBC, CNN, NBC, and ABC. For information about ePolicy Institute products and services, including Fill-in-the-Blanks ePolicy & Social Media Policy Forms Kits, contact 614-451-3200 or nancy@epolicyinstitute.com.