WHITE PAPER: ACCEPTABLE USAGE POLICY

AUPs for Web 2.0:

Creating Effective Policies to Manage Use & Mitigate Risks

by Nancy Flynn
Founder & Executive Director, The ePolicy Institute

Author, Handbook of Social Media (2011), The e-Policy Handbook, E-Mail Rules, Instant Messaging Rules, Blog Rules, Writing Effective E-Mail, and E-Mail Management

Symantec.cloud

White Paper: Acceptable Usage Policy

AUPs for Web 2.0:

Creating Effective Policies to Manage Use & Mitigate Risks

Contents

Overview

Symantec.cloud, www.symanteccloud.com, and The ePolicy Institute™, www.epolicyinstitute.com, have created **AUPs for Web 2.0: Creating Effective Policies to Manage Use and Mitigate Risks**, a best practices-based business guide for compliance officers, IT decision-makers, security managers, and anyone who plays a role in managing—and mitigating—legal, regulatory, and security risks in the workplace.

Through the implementation of a strategic compliance management program, incorporating clear and comprehensive Acceptable Usage Policies, formal employee education, and a proven-effective SaaS solution, employers can quickly and cost-effectively manage their legal, regulatory, security, and other organizational obligations, challenges, and risks.

AUPs for Web 2.0: Creating Effective Policies to Manage Use and Mitigate Risks 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, Symantec.cloud, is engaged in rendering advice on legal, regulatory, or other issues. Before acting on any practice, policy, or procedure addressed in this whitepaper, you should consult with legal counsel or other professionals competent to review the relevant issue.

Introduction: 21st Century Tools Require 21st Century Rules

From Twitter and Facebook, to blogs and YouTube, to private email accounts and personal technology tools, employees' access to the Web—and employers' exposure to potentially costly and protracted risks—is greater today than ever before.

Activities such as surfing news sites for sports scores, paying personal bills online, responding to customer inquiries via Twitter, and promoting business products and services on Facebook increase organizations' exposure to risks. These risks can present themselves in the form of lawsuits, regulatory violations, security breaches, mismanaged business records, productivity drains and public relations disasters.

When employed strategically, there's no denying that business blogs, corporate Facebook accounts, instructional YouTube videos, and other online tools can facilitate speedy two-way communication with customers and prospects. Similarly, when managed properly, personal use of the company's computer system can enhance employees' overall satisfaction with and commitment to their jobs.

At the end of the day, employers must perform a balancing act. On the one hand, you want to provide enough Web access to keep your business thriving and maintain consideration for some level of personal usage. On the other hand, you are obligated to manage Web use in order to protect the organization's assets, reputation, and future. The most effective way to accomplish both goals: implement Acceptable Usage Policies (AUPs) supported by comprehensive employee training and enforced by best-in-class technology.

Our Relationship with Technology Is Evolving

As technology has evolved, so too has our relationship with it. Not too long ago, it was fairly common for organizations to impose across-the-board bans on non-business-related Web surfing, private email accounts, and personal technology tools in the workplace. Banning personal use is no longer a recommended best practice for most organizations. With the exception of the financial services industry and other heavily regulated businesses that must restrict access for security reasons, it simply is not realistic in 2011 to prohibit *all* access to *all* private accounts and *all* personal tools.

Employees—particularly younger employees who have grown up online—expect ready access to email, the Web, and social media, both for business and personal use. Impose a strict ban on texting and Tweeting, blogging and surfing, and you're likely to find your workers seeking employment elsewhere. The cost of replacing experienced staff with untrained employees can be staggering, even in a tight economy with high unemployment.

The goal is to marry your employees' desire for access with your organization's need to maximize compliance while minimizing risks. In other words, establish 21st century rules to govern employee use of 21st century tools.

AUPs Will Never Go Out of Style

While technology continues to evolve, one fact of strategic compliance management will never change. Best practices always have—and always will—call for the establishment and enforcement of AUPs designed to maximize compliance with legal, regulatory, security, and organizational rules—while minimizing business and user risks. Regardless of your organization's industry, size, or status as a public or private entity, you must impose AUPs governing email and Web use, content, and business record retention.

Recommended Best Practice: Conduct an AUP Audit

Just a few months into 2011, the time is right to take a comprehensive, clear-eyed look at your organization's AUP program. In other words, conduct an AUP audit. An effective AUP audit should include the following:

1. Review current federal and state laws governing content, usage, monitoring, privacy, eDiscovery, data encryption, and other legal issues in all states in which you operate, have customers, or litigate lawsuits.
2. Evaluate federal and state, industry and government regulations governing content, use, data security, customer data, patient privacy, and business records.
3. Review all organizational and data security risks facing your company, customers and employees.
4. Evaluate the ways in which your organization uses technology.
5. Evaluate employees' personal use of the company's computer system.
6. Review all existing AUPs.

Based on the findings of your comprehensive AUP audit, you are now ready to update old policies and, as necessary, create new AUPs. Remember, you want to maximize communication and compliance by establishing one free-standing policy per technology. To do this, date each new AUP and collect and destroy all but one file copy of your old policies. Also, make sure every employee receives one copy of each new AUP. This process should be repeated annually.

To assist you in conducting your AUP audit, an AUP audit questionnaire has been included at the end of this whitepaper (see Appendix A).

Essential Rules for Effective AUPs

Effective AUPs incorporate rules governing usage, content, and business record retention. The results of your AUP audit will help you understand the specific risks facing your organization, and will facilitate the establishment of effective rules and policies for your users. In addition to any organization-specific guidelines you may impose, best practices call for the adoption of formal rules governing personal use of email and the Web, as well as comprehensive content rules.

Personal Use Demands Clear and Specific Rules

When it comes to personal use of email, Web, social media, and other company technology resources, you must draft clear and specific rules that are not open to individual interpretation. It's not enough to say that employees are allowed a "limited amount of appropriate, personal computer use." To some employees, "appropriate, personal use" may mean hours devoted to surfing the Web, posting on Facebook, and emailing buddies. 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.

Use your email 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 AUP allows for authorized personal email, those personal messages will be monitored and may be retained along with business-related

email. Employees 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.

Once your personal email and Web use rules are in place, use training and technology, including SaaS content control, to help enforce compliance.

Banning & Blocking Sites Is Increasingly Challenging

Use your Web policy to clarify what type of personal, non-business-related websites employees may—and may not—visit. You might, for example, allow employees to conduct online banking or visit news sites. On the other hand, you may want to ban visits to "controversial" sites related to politics or religion, for example.

If it's been awhile since your organization established a list of "banned and blocked" websites (by content type and/or URL), now is the time to revisit the issue. Banning and blocking sites today is a complex and time-consuming task. The Web is more crowded than ever, thanks to blogs, social media, the shift toward online news, the introduction of eBooks, and the seemingly non-stop growth of online content.

Once you have researched and determined your 2011 list of banned sites, use training and technology, including SaaS URL blocks, to help enforce compliance.

Apply Content Rules to Enforce Legal & Regulatory Compliance

Social media and increased online activity (business and personal) have ushered in a "new era" of Web-related litigation and regulatory violations. No longer are workplace lawsuits and regulatory audits restricted to inappropriate email use and unmanaged Web surfing. Employees today are using smartphones to send "sext" messages, including obscene photos and off-color text, to coworkers. Angry workers are using Twitter and blogs to defame customers and malign managers. Resentful ex-employees and poorly trained staff are using YouTube and Facebook to reveal company secrets, gossip about patients, and expose consumer data. Still others are using email and IM to (accidentally or intentionally) transmit inappropriate, illegal, or otherwise objectionable content.

As a result, employers face increased exposure to lawsuits including hostile work environment and defamation claims, as well as regulatory investigations and fines stemming from violations of the Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), and other regulatory guidelines designed to protect consumer data.

When it comes to content control, best practices call for the implementation of AUPs that incorporate clear content rules governing employees' business and personal use of email, IM, the Web, social media, text messages, and other electronic business communication tools. Use formal content rules to outlaw text, photos, videos, art, or other content that could trigger legal claims, serve as smoking gun evidence of wrongdoing, or violate regulators' content rules.

Best practices call for the inclusion of the following content rules, among others, into your organization's updated 2011 AUPs:

- 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) policy breaches.

Adhere to best practices. Enforce your organization's content rules and AUPs with policy-based SaaS technology. Symentec.cloud, for example, delivers Content Control, Image Control, and Web URL Filtering to quickly and automatically:

- Search target words and phrases that violate AUPs and content rules.
- Monitor use (business and personal) and filter policy violations to prevent inappropriate and otherwise offensive content from entering or leaving your system.
- Block banned websites, including selected social media, to stop bad behavior before it starts.

Support AUPs with Education: 10 Tips for Effective AUP Training

Now that you've updated your organization's AUPs, it's time to educate your workforce about risks and rules, policies and procedures. You cannot expect an untrained workforce to be a compliant workforce, so educate everyone, from the summer intern to the CEO. Ten tips for effective AUP training:

1. Approach AUP training as an ongoing, continuing education program, not a one-time event.
2. Review email, Web, and other electronic risks with employees. Recap the legal, regulatory, security, productivity, public relations, and career risks facing individual users and the organization.
3. Adhere to the company's content rules. Remind users that the easiest way to control risk is to control written content.
4. Stress the fact that a policy is a policy. Make sure employees understand that all AUPs and other employment policies (including ethics rules, harassment and discrimination guidelines, confidentiality rules, etc.) apply 24/7 at work, home, and on the road.

5. Educate employees about trade secrets and confidential data. Explain the legal and regulatory risks facing the company if customers' financial data or patients' electronic protected health information is breached, or company secrets are revealed.
6. Review monitoring policies and procedures. Discuss First Amendment and privacy expectations and realities.
7. Define "electronic business record" and share the organization's record retention policy and procedures.
8. Define "personal use." Let employees know with whom, under what circumstances, and during what periods of the day it is acceptable.
9. Provide every employee with one copy of each AUP.
10. Require all employees to sign and date acknowledgement forms attesting that they understand your AUPs and will adhere to them, or face the consequences, up to and including termination.

Enforce AUPs with SaaS Technology

An essential, best-practices-based tool, SaaS is essential to every organization's AUP program. SaaS helps facilitate AUP compliance by:

- **Minimizing Legal Risks.** SaaS Content Control and URL Blocks reduce the likelihood of litigation by controlling potentially damaging email content and blocking banned Web images. SaaS Archiving ensures your ability to preserve, protect, and produce legally compliant email and other electronic business records.
- **Reducing Regulatory Risks.** SaaS Encryption, Email Continuity, and Antivirus Protection services help keep customers' private data, patients' electronic protected health information (EPHI), company financials, and other confidential data securely under wraps. SaaS Email Content Control Filtering and Archiving help keep you compliant with regulators' content and record retention rules.

Symantec.cloud Supports AUPs for Web 2.0

Symantec.cloud is a management platform that helps IT executives administer, monitor, and protect enterprise data resources and endpoints more thoroughly. Their portfolio of services offers a platform for managing technologies that:

- Address the business requirements for a secure computing environment.
- Enable consistent application of acceptable use and regulatory policies.
- Provide ongoing access to critical applications such as email to ensure high levels of productivity.

Symantec MessageLabs Policy Based Encryption.cloud

The Policy Based Encryption.cloud service is a fast and easy way to implement an email encryption solution to help ensure compliance with federal and state law along with industry rules and regulations. This flexible solution allows you to create and enforce customized policies for your particular requirements. SaaS technology can encrypt messages—automatically, instantly, securely—based on sender and recipient information, or detailed scans of email content and attachments for words, names, phrases, numbers, and file types. Recipients of encrypted email can easily access messages without any special knowledge. IT management and costs are significantly reduced, as key management is handled by Symantec.cloud. The solution is simple to set-up, configure, and use.

Symantec MessageLabs Email Archiving.cloud

The courts appreciate consistency. If you can demonstrate that your organization has consistently applied clear email usage, content, and retention policies—supported by comprehensive employee education and a proven-effective managed email archiving service—then the court is more likely to look favorably upon your organization should you one day find yourself embroiled in a workplace lawsuit. The Email Archiving.cloud service provides you with a proven email archiving solution that meets your needs for mailbox management, eDiscovery, email compliance, and supervision. High-performance search, using Symantec.cloud's advanced distributed search architecture, means archived email can be retrieved in seconds, regardless of storage size.

Summary: AUPs for Web 2.0

The ever-expanding universe of technology tools facilitates users' ability to quickly and conveniently transmit business-critical data and stay connected with colleagues and customers around the globe. That's the good news. The bad news: new and emerging technologies dramatically increase employers' exposure to potentially costly and protracted risks, including workplace lawsuits, regulatory fines, security breaches, and productivity drains, among others.

Fortunately, for savvy employers determined to manage technology use and minimize risks, there is a solution. Through the strategic implementation of a comprehensive Acceptable Usage Policy program combined with formal employee education, supported by SaaS technology, organizations can successfully manage (and in some cases prevent) legal, regulatory, security, and productivity risks, while maximizing compliance.

About The ePolicy Institute™

www.epolicyinstitute.com

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 *Handbook of Social Media* (2011 Pfeiffer) and *The e-Policy Handbook, 2nd Edition*, Founder and Executive Director Nancy Flynn is an in-demand trainer, consultant, and expert witness. Since 2001, ePolicy Institute has collaborated with American Management Association on annual surveys of workplace email/Internet policies, procedures, 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, CBS, CNBC, CNN, NBC, and ABC. For information about ePolicy Institute products and services, contact 614-451-3200 or nancy@epolicyinstitute.com.

Appendix A: AUP Audit Questionnaire

Legal Risks & Compliance

1. Have you reviewed current federal and state laws governing electronic content, usage, monitoring, privacy, eDiscovery, data encryption, and other legal issues in all states in which you operate, have customers, or litigate lawsuits?

   Yes No Don't Know

2. Has employee email ever triggered a workplace lawsuit?

   Yes No Don't Know

3. Have inappropriate blog posts or offensive social media content (Tweets, Facebook posts, YouTube videos, etc.) ever triggered a workplace lawsuit?

   Yes No Don't Know

4. Has employee Web use (surfing, downloading, etc.) ever triggered a workplace lawsuit?

   Yes No Don't Know

eDiscovery Risks & Compliance

5. Has employee email ever been subpoenaed by a court or regulatory body?

   Yes No Don't Know

6. Has email or other electronic stored information (ESI) ever been used as evidence—for or against your company—in litigation?

   Yes No Don't Know

7. Have you provided employees with a formal definition of "electronic business record"?

   Yes No Don't Know

8. Do your employees know the difference between business-critical email that must be retained vs. insignificant messages that may be purged?

   Yes No Don't Know

9. Do you rely on archiving technology to automatically preserve, protect, and produce legally compliant email and other ESI?

Yes No Don't Know

10. Could you locate and produce legally compliant email and other ESI in 99 days if ordered by the court to do so?

Yes No Don't Know

Regulatory Risks & Compliance

11. Do you know and understand all the regulations (federal, state, industry, government) that govern your organization's electronic use, content, records, data security, customer data, patient privacy, and eDiscovery obligations?

Yes No Don't Know

12. Have you educated regulated employees about electronic risks and compliance?

Yes No Don't Know

Organizational & Productivity Risks & Compliance

13. Has excessive personal use of *email* led to a slide in workplace productivity?

Yes No Don't Know

14. Has excessive personal use of the *Web* led to a slide in workplace productivity?

Yes No Don't Know

15. Has excessive personal use of *social media* led to a slide in workplace productivity?

Yes No Don't Know

16. Have you ever terminated an employee for violating *email* policy?

Yes No Don't Know

17. Have you ever terminated an employee for violating *Web* policy?

Yes No Don't Know

18. What does your company consider to be a termination-worthy email or Web violation? (Check all that apply)

- ☐ Violation of any company policy
- ☐ Inappropriate or offensive language or content
- ☐ Excessive personal use
- ☐ Breach of confidentiality rules
- ☐ Other

Security Risks & Compliance

19. Are telecommuters, remote workers, and mobile users accessing the Web outside the security of your corporate network?

Yes No Don't Know

20. Has your organization ever been attacked by hackers or cybercriminals?

Yes No Don't Know

21. Have leaked internal email messages ever triggered negative media coverage, a drop in stock valuation, a regulatory audit, or other negative consequences?

Yes No Don't Know

22. Has compromised customer data ever put you at risk of GLBA violations?

Yes No Don't Know

23. Have cybercriminals ever launched phishing attacks against your IT system?

Yes No Don't Know

24. Has HIPAA-protected electronic health information ever been exposed—accidentally or intentionally—to outside third-parties?

Yes No Don't Know

Personal Use

25. Do employees use their own personal blogs and social networking sites to comment on your business, employees, executives, customers, products & services?

Yes No Don't Know

26. Do employees use their own personal blogs and social networking sites to gossip, whine, or complain about your business, employees, executives, customers, products & services?

Yes No Don't Know

27. On their own time and using their own computer equipment, have employees ever—accidentally or intentionally—leaked confidential company, consumer, or patient information that has triggered a regulatory investigation, sparked a lawsuit, or damaged the organization's reputation?

Yes No Don't Know

28. Do you monitor employees' personal blogs and personal social networking sites?

Yes No Don't Know

Business Use

29. Does your organization use social media externally to interact with customers and prospects, vendors and decision-makers, shareholders and the media?

Yes No Don't Know

30. Does your organization use social media internally for knowledge-sharing and two-way communication among employees?

Yes No Don't Know

31. Do you maintain a business blog?

Yes No Don't Know

32. Do you have a corporate social media presence on Facebook, Twitter, YouTube, etc?

Yes No Don't Know

33. Do you provide employees with BlackBerries or smartphones?

Yes No Don't Know

34. Are employees allowed to use company-provided BlackBerries/smartphones for personal reasons?

Yes No Don't Know

35. On average, how much personal use of the company system do employees engage in daily?

- ☐ 0-30 minutes
- ☐ 30 minutes – 2 hours
- ☐ 2 hours – 4 hours
- ☐ 4+ hours

36. When it comes to blocking Web access, what type of sites is your company most concerned about? (Check all that apply.)

- ☐ "Adult" sites with sexual/pornographic/romantic content
- ☐ Game sites
- ☐ Shopping/auction sites
- ☐ News sites
- ☐ Entertainment sites
- ☐ Sports sites
- ☐ Social media sites
- ☐ External blog sites

37. Do you provide employees with access to IM for internal/external communication?

Yes No Don't Know

38. Do employees use text messaging for internal/external communication?

Yes No Don't Know

39. Does your technology support roaming and remote workers, safeguarding your system and secrets regardless of geographic location?

Yes No Don't Know

AUP Program Review

40. What AUPs does your organization currently have in place? (Check each separate, free-standing policy that applies.)

- ☐ Business record retention
- ☐ Email use & content (business-related)
- ☐ Email use & content (personal)
- ☐ Web use & content (business-related)
- ☐ Web use & content (personal)
- ☐ Social media use & content (business-related)
- ☐ Social media use & content (personal)
- ☐ Blog use & content (business-related)
- ☐ Blog use & content (personal)
- ☐ IM use & content (business-related)
- ☐ IM use & content (personal)
- ☐ Texting use & content (business-related)
- ☐ Texting use & content (personal)
- ☐ BlackBerry/smartphone use & content (business-related)
- ☐ BlackBerry/smartphone use & content (personal)

41. Have all your AUPs been reviewed and updated (as necessary) within the past 12 months?

Yes No Don't Know

42. Are your AUPs easy to read, understand, and adhere to?

Yes No Don't Know

43. How do you distribute AUPs to employees? (Check all that apply.)

- ☐ Employee handbook
- ☐ Company Intranet
- ☐ Email
- ☐ Formal AUP training

44. Are all employees required to complete formal AUP training?

Yes No Don't Know

45. Do you clearly date each new AUP?

Yes No Don't Know

46. Do you take old AUPs out of circulation before distributing new AUPs?

Yes No Don't Know

47. In the event of a lawsuit, are you confident that you could demonstrate to the court that your organization has established a best practices-based AUP program that combines effective policies, supported by comprehensive employee education and enforced by best-in-class technology?

Yes No Don't Know

More Information

AMERICAS

UNITED STATES
512 Seventh Avenue
6th Floor
New York, NY 10018
USA
Toll-free +1 866 460 0000

CANADA
170 University Avenue
Toronto, ON M5H 3B3
Canada
Toll-free :1 866 460 0000

EUROPE

HEADQUARTERS
1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom
Tel +44 (0) 1452 627 627
Fax +44 (0) 1452 627 628
Freephone 0800 917 7733

LONDON
3rd Floor
40 Whitfield Street
London, W1T 2RH
United Kingdom
Tel +44 (0) 203 009 6500
Fax +44 (0) 203 009 6552
Support +44 (0) 1452 627 766

NETHERLANDS
WTC Amsterdam
Zuidplein 36/H-Tower
NL-1077 XV
Amsterdam
Netherlands
Tel +31 (0) 20 799 7929
Fax +31 (0) 20 799 7801

BELGIUM/LUXEMBOURG
Symantec Belgium
Astrid Business Center
Is. Meyskensstraat 224
1780 Wemmel,
Belgium
Tel: +32 2 531 11 40
Fax: +32 531 11 41

DACH
Humboldtstrasse 6
Gewerbegebiet Dornach
85609 Aschheim
Deutschland
Tel +49 (0) 89 94320 120
Support :+44 (0)870 850 3014

NORDICS
St. Kongensgade 128
1264 Copenhagen K
Danmark
Tel +45 33 32 37 18
Fax +45 33 32 37 06
Support +44 (0)870 850 3014

ASIA PACIFIC

HONG KONG
Room 3006, Central Plaza
18 Harbour Road
Tower II
Wanchai
Hong Kong
Main: +852 2528 6206
Fax: +852 2526 2646
Support: + 852 6902 1130

AUSTRALIA
Level 13
207 Kent Street,
Sydney NSW 2000
Main: +61 2 8220 7000
Fax: +61 2 8220 7075
Support: 1 800 088 099

SINGAPORE
6 Temasek Boulevard
#11-01 Suntec Tower 4
Singapore 038986
Main: +65 6333 6366
Fax: +65 6235 8885
Support: 800 120 4415

JAPAN
Akasaka Intercity
1-11-44 Akasaka
Minato-ku, Tokyo 107-0052
Main: + 81 3 5114 4540
Fax: + 81 3 5114 4020
Support: + 852 6902 1130

About Symantec.cloud

More than 31,000 organizations ranging from small businesses to the Fortune 500 across 100 countries use Symantec.cloud to administer, monitor, and protect their information resources more effectively. Organizations can choose from 14 pre-integrated applications to help secure and manage their business even as new technologies and devices are introduced and traditional boundaries of the workplace disappear. Services are delivered on a highly scalable, reliable and energy-efficient global infrastructure built on fourteen datacenters around the globe. A division within Symantec Corporation, Symantec.cloud offers customers the ability to work more productively in a connected world.

For specific country offices and contact numbers, please visit our website.

Symantec.cloud North America
512 7th Ave.
6th Floor
New York, NY 10018 USA
1 (646) 519 8100
1 (866) 460 0000
www.SymantecCloud.com

Symantec helps organizations secure and manage their information-driven world with **managed services**, **exchange spam filter**, **managed security services**, and **email antivirus**.

3/2011 21179198