

Table of Contents

Table of Contents	0
1 Introduction.....	7
1.1 Purpose.....	7
1.2 Intended Audience.....	7
1.3 Internet Background.....	7
1.4 Why create Security Policy for Internet-Related Issues?.....	7
1.5 Major Types of Policy.....	8
2 General Policy	11
2.1 What to Include.....	11
2.2 Obtaining Approval	11
2.3 Getting Policy Implemented	12
2.4 Sample High Level Policy Statements.....	13
3 Risk Profiling.....	15
3.1 Threats/Visibility.....	15
3.2 Sensitivities/Consequences.....	17
3.3 Profile Matrix.....	17
3.4 Information Asset Inventory.....	18
3.5 General Support Systems	18
3.6 Critical/Major Applications.....	19
3.7 Data Categorization	19
4 Business Requirements	21
4.1 Remote Access.....	22
4.2 Dial-in.....	23
4.3 Telnet/X Windows.....	24
4.4 Mobile Computing.....	24
4.5 Electronic Mail	25
4.6 Information Publishing.....	25
4.7 Research	26
4.8 Electronic Commerce.....	27
4.9 Electronic Data Interchange	27
4.10 Information Transactions.....	28
4.11 Financial Transactions	28
4.12 High Availability	29
4.13 Ease of Use	30
4.14 Single Sign-on	30
4.15 User Interface Design	31
5 Sample Policy Areas.....	33
5.1 Identification and Authentication.....	33
5.1.1 General Internet I&A Policies	34
5.1.2 Password Management Policies.....	35
5.1.3 Robust Authentication Policy.....	36
5.1.4 Digital Signatures and Certificates.....	36
5.2 Software Import Control	37
5.2.1 Virus Prevention, Detection, and Removal.....	38
5.2.2 Controlling Interactive Software.....	42
5.2.3 Software Licensing.....	45
5.3 Encryption.....	46
5.3.1 General Encryption Policy	46
5.3.2 Remote Access.....	48
5.3.3 Virtual Private Networks	49
5.4 System/Architecture Level.....	49
5.4.1 Virtual Private Networks.....	49
5.4.2 Remote System Access	51

5.4.3	Access to Internal Databases	52
5.4.4	Use of Multiple Firewalls	53
5.5	Incident Handling	54
5.5.1	Intrusion Detection Overview.....	54
5.5.2	Methods.....	55
5.5.3	Incident Response	57
5.6	Administrative	60
5.6.1	Assigning Security Responsibility	60
5.6.2	Appropriate Use	61
5.6.3	Privacy.....	64
5.7	Awareness and Education.....	64
6	Internet Firewall Policy	67
6.1	Background and Purpose.....	67
6.2	Authentication.....	67
6.3	Routing Versus Forwarding.....	68
6.3.1	Source Routing	68
6.3.2	IP Spoofing	68
6.4	Types of Firewalls.....	68
6.4.1	Packet Filtering Gateways.....	68
6.4.2	Application Gateways.....	69
6.4.3	Hybrid or Complex Gateways.....	70
6.4.4	Rating	70
6.5	Firewall Architectures.....	70
6.5.1	Multi-homed host	70
6.5.2	Screened host.....	71
6.5.3	Screened subnet.....	71
6.6	Intranet	71
6.7	Firewall Administration.....	71
6.7.1	Qualification of the Firewall Administrator.....	72
6.7.2	Remote Firewall Administration	72
6.7.3	User Accounts.....	73
6.7.3.1	Firewall Backup.....	73
6.8	Network Trust Relationships.....	73
6.9	Virtual Private Networks (VPN)	74
6.10	DNS and Mail Resolution	74
6.11	System Integrity	75
6.12	Documentation.....	75
6.13	Physical Firewall Security.....	75
6.14	Firewall Incident Handling	75
6.15	Restoration of Services	76
6.16	Upgrading the firewall	76
6.17	Revision/Update of Firewall Policy	77
6.18	Logs and Audit Trails (Audit/Event Reporting and Summaries)	77
6.19	Example Policies.....	77
6.20	Example Service-Specific Policies.....	79
6.21	Manager	80
6.22	Technical	80
7	World Wide Web (WWW).....	85
7.1	Browsing the Internet	85
7.2	Example Browsing Policies	85
7.3	Web Servers.....	87
7.4	Example Web Server Policies	88
8	Electronic Mail	91
8.1	Email Usage	91
8.2	Email Primer.....	91
8.2.1	SMTP	91

8.2.2	POP.....	92
8.2.3	IMAP	92
8.2.4	MIME.....	92
8.3	Potential Email Problems.....	92
8.3.1	Accidents.....	92
8.3.2	Personal Use	93
8.1.3	Marketing.....	93
8.4	Email Threats.....	93
8.4.1	Impersonation	94
8.4.2	Eavesdropping.....	94
8.4.3	Mailbombing	94
8.4.4	Junk and Harassing Mail.....	94
8.5	Email Safeguards.....	95
8.5.1	Impersonation	95
8.5.2	Eavesdropping.....	95
8.6	Acceptable Use Of Electronic Mail	95
8.7	Protection of Electronic Mail Messages and Systems.....	95
8.8	Example Email Policy	96
8.9	Retention of Electronic Mail Messages.....	97
8.9.1	Retention Policy for Federal Agencies.....	98
8.9.2	Commercial Retention Policy	99
	Appendix 1 – Resources for Internet Security Information	101
1.1	Web Sites	101
1.2	Ftp Sites	102
1.3	Usenet News Groups.....	103
1.4	Mailing Lists.....	103
1.5	Books	104
	Appendix 2 – Glossary	107

