Technology Policies and Procedures: Protecting Client and Program Data

Donald G. Carder
Atlanta Legal Aid Society
Michael T. Bowen
Community Legal Services of Philadelphia

TIG Conference January 12-15, 2010 Austin, TX

Why Have a Policy?

- Federal Regulations
- Responsibility to the Internet
- Document Program Procedures
- Mitigate Liability and Protect Protect Client Confidentiality

A Little Paranoia
Can Be a Good Thing

- Client Confidentiality is Critical to Staying in Business.
- More and More Client Data is Finding its Way Online.
- In 2009, More Than 220 Million Client Records Were Exposed.
- When it Comes to Technology, Legal Services Programs in General are Traditionally Underfunded, and Understaffed
- You ARE Being Targeted

Purpose of Policies

- Not Just “Rules and Regulations”
- Protective Tools
- Ensure Employees are on the Same Operational Page

Types of Policies

- Point Specific - Cover a single areas such as “Acceptable Use”
- Standards - Collections of of system-specific or procedural-specific requirements such as workstation configurations.
- Guidelines - Suggestions for “Best Practices”

Preparation and Planning

- Identify Areas of Concern
- Create Stakeholder Committees
- Acknowledge Politics

Policy Elements

- Scope
- Definitions
- Declaration of Responsibility
- Enforcement Clauses

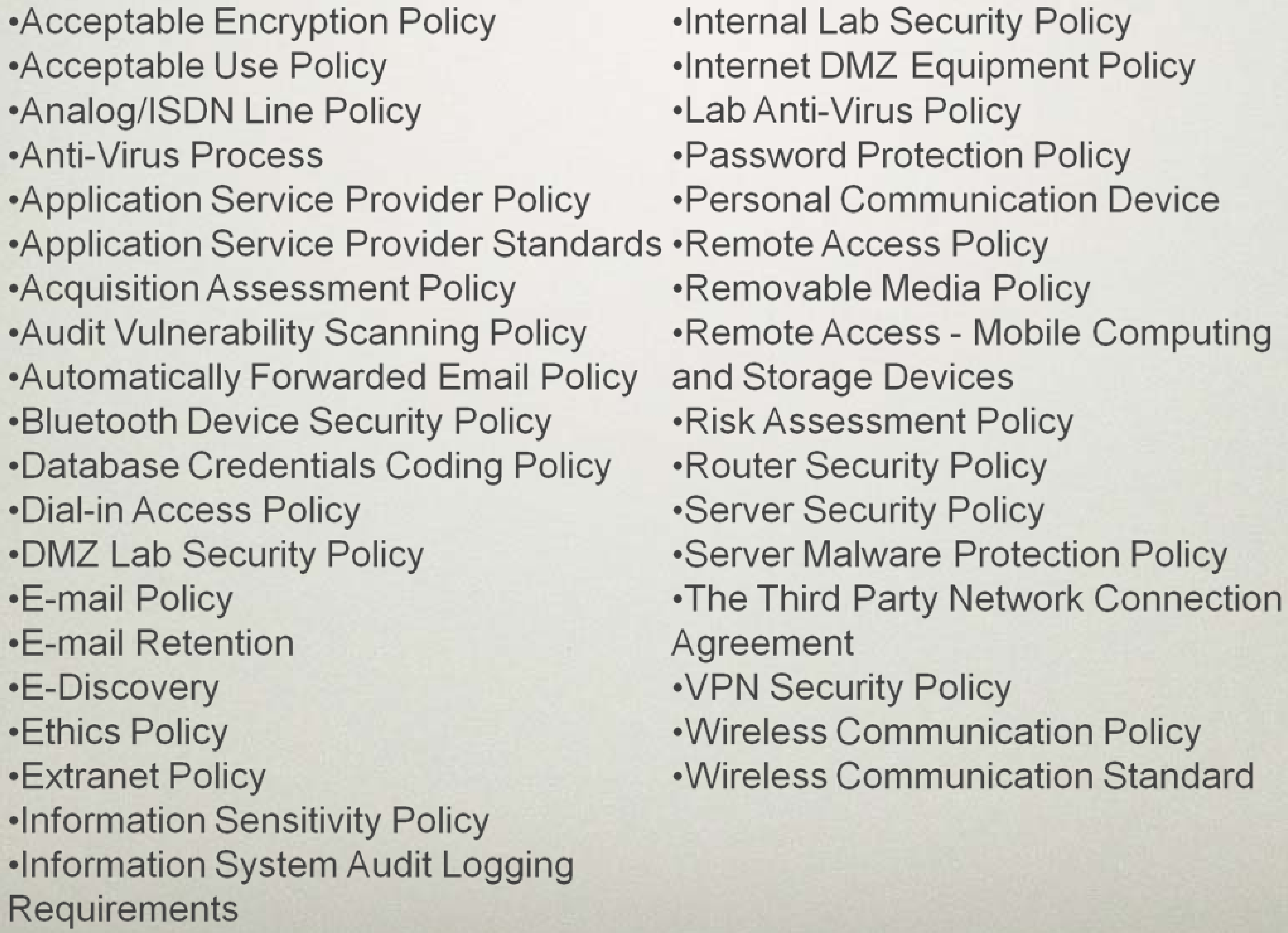
Special Note: Client Confidentiality

- Clearly Define What is to be Considered “Confidential”
- Establish Controls for the Protection of Confidential Data (e.g., Encryption
- Establish Guidelines for Data Exchange
- Beware of Data Aggregators

Implementation

- Incorporate into Program Manuals
- Get Signatures
- Address Technical Concerns
- Policies are “Living Documents” - Revise and Refine as Necessary
- Ongoing Awareness is Crucial

Sample Policies From The SANS Security Policy Project:
http://www.sans.org/security-resources/policies/



- Acceptable Encryption Policy
- Acceptable Use Policy
- Analog/ISDN Line Policy
- Anti-Virus Process
- Application Service Provider Policy
- Application Service Provider Standards
- Acquisition Assessment Policy
- Audit Vulnerability Scanning Policy
- Automatically Forwarded Email Policy
- Bluetooth Device Security Policy
- Database Credentials Coding Policy
- Dial-in Access Policy
- DMZ Lab Security Policy
- E-mail Policy
- E-mail Retention
- E-Discovery
- Ethics Policy
- Extranet Policy
- Information Sensitivity Policy
- Information System Audit Logging Requirements
- Internal Lab Security Policy
- Internet DMZ Equipment Policy
- Lab Anti-Virus Policy
- Password Protection Policy
- Personal Communication Device
- Remote Access Policy
- Removable Media Policy
- Remote Access - Mobile Computing and Storage Devices
- Risk Assessment Policy
- Router Security Policy
- Server Security Policy
- Server Malware Protection Policy
- The Third Party Network Connection Agreement
- VPN Security Policy
- Wireless Communication Policy
- Wireless Communication Standard