



PRIVACY AUDIT REPORT

SAMPLE REPORT

This is a preview of the report you will receive after your privacy audit. The report contains detailed explanations of each section of the privacy regulation, along with our findings on what changes you should make to bring your company into better compliance.

Introduction.....	1
What We Did	2
What We Found.....	4
Secure user authentication.....	5
Control of user IDs.....	5
Password security.....	6
Password storage.....	7
Restricting access to active users	8
Account Lockout.....	9
Secure access control.....	10
Restrict access to files	10
Unique identification	11
Encryption of transmitted information.....	11
Monitoring.....	15
Encryption of laptops and portable devices	15
Firewall and operating system patches.....	16
Firewall protection.....	17
Operating system patches	17
Anti-virus/Anti-malware.....	20
Education/Training.....	22
What You Should Do (Summary)	23

Introduction

On October 31, 2007, the Massachusetts General Law was amended to add Chapter 93H (“Security Breaches”). This law charged the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR) with developing and enforcing regulations to prevent the disclosure of personal information on residents of the commonwealth by businesses to unauthorized people. This law came about in part as a reaction to high-profile breaches of security such as the one in which credit and debit card numbers of more than 45 million customers of TJX (the parent company of such retailers as T.J. Maxx and Marshall’s) were stolen due to insufficient protections on the company’s data.

The Office of Consumer Affairs has developed regulations in accordance with M.G.L. c. 93H. These regulations have been published in the Code of Massachusetts Regulations as 201 CMR 17.00. The regulations present specific legal definitions of terms such as “personal information”; establish a minimum set of procedures that businesses must follow to protect personal information; require that businesses disclose any breaches of security that they become aware of; and creates stiff financial penalties for failure to comply. The regulation defines “personal information” as the name of a Massachusetts resident (first and last name or first initial and last name), and one of the following identifying numbers: social security number, drivers license number, or financial account number (such as bank account or credit card number). This regulation, arguably the most aggressive in the country, will require almost all businesses to make changes to their technology infrastructure and business practices. Due to the far-reaching nature of the regulation and the difficulty of complying, the OCABR has extended the deadline for companies to become compliant several times. Currently, all companies must be compliant by March 1, 2010.

Section 17.04 of the regulation (“Computer System Security Requirements”) establishes specific requirements for the protection of personal information stored electronically. Atlas Technology Consulting provides many services to help clients like you improve your technology infrastructure to move towards compliance with this section of the regulation.

The first step in helping your organization was an in-depth investigation into the current state of computer system security within the organization, in the form of an on-site audit (along with a pre-audit survey). Atlas has analyzed the results of this audit and this report contains the steps we recommend you take.