Storing electronic information while maintaining compliance.

ATA Technologies

Daniel Simons

Michael Laffoon

www.atacpatech.net

About ATA Technologies

Our mission is simple: Deliver technology services, so our clients can focus on their businesses

- Network Management
  - Wide & Local Area Networking
  - Wireless
- Business Solutions
  - Hardware & Software Solutions
  - Technology Assessments
  - Remote Access
- Disaster Recovery
  - Offsite Backup Services
- Security Solutions
- Antivirus Solutions
- IT Auditing
- Computer Forensics

What establishes requirements for compliance?

- Federal law
  - Clean Water Act, the ***National Pollutant Discharge Elimination System*** (***NPDES***)
- State law
  - Tenn. Admin Rule 1200-5-1
- Precedent
  - Court cases

What establishes requirements for compliance?

- Standards
  - Payment Card Industry Data Security Standard (PCI-DSS)
- Recommendations
  - *Internal Control and Compliance Manual for Tennessee Municipalities*

Penalties of Non-Compliance

- Cease and desist orders
- Civil monetary penalty
- Court injunction
- Criminal monetary penalty
- Imprisonment

Penalties of Non-Compliance

- License modification order
- Limitations on activities, functions, and operations
- Modification or termination of contract
- Registration revocation
- Revocation order
- Suspension order

THE UNIVERSITY of TENNESSEE

MUNICIPAL TECHNICAL ADVISORY SERVICE

In cooperation with the Tennessee Municipal League

RECORDS MANAGEMENT FOR MUNICIPAL GOVERNMENTS

... a reference guide for city officials and municipal public records custodians

January 2009

Dennis Huffer, Legal Consultant

S. Utilities (Billing and Collection)

DESCRIPTION OF RECORD	RETENTION PERIOD	LEGAL AUTHORITY/RATIONALE
S-1. Applications for Service. Customer requests for service, including name, address, phone, services, and signatures.	Retain 3 years after service is discontinued but may want to keep in electronic format longer in case customer returns to service.	Keep in case of billing errors. Tennessee courts have allowed utilities to back bill customers 3 years.
S-2. Audit Reports. Independent audit of financial records.	Permanent record.	Recommended by the comptroller in the *Internal Control and Compliance Manual for Tennessee Municipalities*.
S-3. Billing Adjustment Reports. Customer names and adjustment information.	Retain 3 years.	Keep in case of billing errors. Tennessee courts have allowed utilities to back bill customers 3 years.
S-4. Billing Stubs. Collection stubs of accounts paid.	Retain 3 years.	Keep in case of billing errors. Tennessee courts have allowed utilities to back bill customers 3 years.

DESCRIPTION OF RECORD	RETENTION PERIOD	LEGAL AUTHORITY/RATIONALE
S-5. Billing Register. Listing of monthly customer billings (account number, amount, etc.).	Retain 7 years. If record kept in electronic format, the paper copy may be destroyed after audit.	Keep to help resolve billing disputes with customers.
S-6. Collection Agency Reports. Listing of accounts turned over for collection and how resolved.	Retain 7 years.	Keep to help resolve billing disputes with customers.
S-7. Complaints by Customers. Records of meter rechecks, billing inquiries, service problems, etc.	Retain 5 years.	Keep in case of litigation.
S-8. Deposits from Customers. Customer name, date, services, amount of deposit.	Retain 3 years after service is discontinued and deposit applied or refunded.	Keep in case of billing errors. Tennessee courts have allowed utilities to back bill customers 3 years.
S-9. Disconnection Notices. Notice to discontinue service after non-payment of bill.	Retain 3 years.	Keep in case of billing errors. Tennessee courts have allowed utilities to back bill customers 3 years.

DESCRIPTION OF RECORD	RETENTION PERIOD	LEGAL AUTHORITY/RATIONALE
S-10. General Ledger. Financial information of the utility. (Also see G-14 and G-21.)	Permanent record. If maintained in electronic format may destroy paper record after 7 years. NOTE: The Tennessee State Library and Archives does not favor keeping permanent records in electronic format.	Recommended by the comptroller in the *Internal Control and Compliance Manual for Tennessee Municipalities*.
S-11. Meter Reading Records. Meter sheets or printouts from hand-held devices.	Retain 3 years.	Keep in case of billing errors. Tennessee courts have allowed utilities to back bill customers 3 years.
S-12. Meter Records. Size, type, meter number, dates service began and ended, serial number.	Retain 1 year after meter is retired and disposed of.	Keep to aid in settling billing disputes involving the accuracy of the meter.
S-13. Meter Tests/Repairs. Record of meter testing and any repairs.	Retain 1 year after meter is retired and disposed of.	Keep to aid in settling billing disputes involving the accuracy of the meter.

DESCRIPTION OF RECORD	RETENTION PERIOD	LEGAL AUTHORITY/RATIONALE
S-14. Rate Schedules. Listing of rates for utility services.	Permanent record.	Keep for historical purposes.
S-15. Tap Records. Including when tap installed, size, location.	Permanent record.	Keep for historical purposes.
S-16. Work Orders for Customer Service. Detail of meter number, installation date, readings, etc.	Retain 3 years.	Keep in case of billing errors. Tennessee courts have allowed utilities to back bill customers 3 years.

T. Utilities (Operation and Maintenance)

DESCRIPTION OF RECORD	RETENTION PERIOD	LEGAL AUTHORITY/RATIONALE
T-1. Bacteriological Records. Records indicating disinfection of mains, tanks, filters, wells.	*Retain 5 years.	Tenn. Admin. Rule 1200-5-1-.17(8).
T-2. Complaint Logs.	*Retain 5 years.	Tenn. Admin. Rule 1200-5-1-.20(1)(h).
T-3. Daily Worksheets and Shift Logs.	*Retain until next sanitary survey.	Tenn. Admin. Rule 1200-5-1-.20 (1)(g).
T-4. Facility Maintenance Records.	*Retain 5 years.	Tenn. Admin. Rule 1200-5-1-.20 (1)(h).

DESCRIPTION OF RECORD	RETENTION PERIOD	LEGAL AUTHORITY/RATIONALE
T-5. Flush and Free Chlorine Residual for New Taps Where Main Is Uncovered, Measurement of.	*Retain until next sanitary survey or 3 years.	Tenn. Admin. Rule 1200-5-1-.17(32).
T-6. Lead and Copper. Original records of all sampling data and analyses, reports, surveys, letters, evaluations, schedules, state determinations, and any other information required by Tenn. Admin. Rules 1200-5-1-.33(2) through (9).	*Retain 12 years.	Tenn. Admin. Rule 1200-5-1-.33(12).
T-7. Underground Utilities, Location of. Record of location of all underground utilities maintained by the city. NOTE: Under T.C.A. § 65-31-105, the city must record location of utilities with county, listing where the facilities are located and the name, title, address, and telephone number of the operator's representative. The county keeps this record permanently.	Permanent record.	These records allow the city to know the location and history of its underground utilities.

U. Utilities (Wastewater and Water Records)

DESCRIPTION OF RECORD	RETENTION PERIOD	LEGAL AUTHORITY/RATIONALE
WASTEWATER RECORDS		
U-1. Discharge Monitoring Reports (DMRs).	Retain 3 years or longer if so requested by Water Pollution Control as a minimum to comply with permit. Retention for life of the facility is recommended.	NPDES Permit Requirements Part I Subpart B.5. Provides record of operations and loading to assist in planning.
U-2. Industrial Pretreatment. All information resulting from monitoring activities.	*Retain 3 years, longer in cases of unresolved litigation.	(40 C.F.R. 403.12(o)(1-3)).
U-3. Laboratory Bench Sheets, Calibration and Maintenance of Instruments, QA/QC Data, Flow Charts.	Retain 3 years or longer if requested by Water Pollution Control.	NPDES Permit Requirements Part I Subpart B.5.
U-4. Land Application of Cumulative Pollutant Loading Rate Sludge under 40 C.F.R. 503.13(a)(2)(I).	*Permanent record.	(40 C.F.R. 503.17(a)(5)(ii)).

DESCRIPTION OF RECORD	RETENTION PERIOD	LEGAL AUTHORITY/RATIONALE
U-5. Monthly Operating Reports (MORs).	Retain 3 years or longer if requested by Water Pollution Control as a minimum to comply with permit. Retention for the life of the facility is recommended.	NPDES Permit Requirements Part I Subpart B.5. Provides record of operations and loading to assist in planning.
U-6. Wastewater Sludge Disposal via Land Application, Surface Disposal, Incineration.	*Retain 5 years.	(40 C.F.R. 503.17) Land Application; (503.27) Surface Disposal; (503.47) Incineration.
DRINKING WATER RECORDS		
U-7. Bacteriological Analysis.	*Retain 5 years.	Tenn. Admin. Rule 1200-5-1-.20 (1)(b).
U-8. Chemical Analysis.	*Retain 10 years.	Tenn. Admin. Rule 1200-5-1-.20 (1)(a).
U-9. Consumer Confidence Reports.	*Retain 5 years.	Tenn. Admin. Rule 1200-5-.35(5)(h).

DESCRIPTION OF RECORD	RETENTION PERIOD	LEGAL AUTHORITY/RATIONALE
U-10. Cross Connection Records.	*Retain 5 years.	Tenn. Admin. Rule 1200-5-1-.20 (1)(h).
U-11. Monthly Operating Reports (MORs).	Retain until next survey at a minimum. Retention for life of the facility is recommended.	Provides record of operations and loading to assist in planning.
U-12. Storage Tank Inspections.	Retain 5 years to comply with rule. Retention for the life of the tank is recommended.	Tenn. Admin. Rule 1200-5-1-.20(1)(h). Retention for life of the tank is recommended to track depreciation and repairs.
U-13. Turbidity. Records include daily worksheets, calibration data, and strip charts.	*Retain until the next sanitary survey.	Tenn. Admin. Rule 1200-5-1-.20(1)(f).
U-14. Variance or Exceptions Granted.	*Retain 5 years following the expiration of such variance or exemption.	Tenn. Admin. Rule 1200-5-1-.20(1)(d).
U-15. Violation, Corrective Action. Records of actions taken to correct violations of primary drinking water regulations.	*Retain 3 years after action.	Tenn. Admin. Rule 1200-5-1-.20(1)(b).
U-16. Written Reports, etc., Related to Sanitary Survey.	*Retain 10 years after sanitary survey.	Tenn. Admin. Rule 1200-5-1-.20(1)(c).

Other types of records

- Email
- Instant message chat
- Customer and employee portals
- Meeting and committee minutes
- Projects
- Voicemail

How long should we retain other records such as email?

- Check with a lawyer for you specific industry and jurisdiction. In general, there is no retention period mandated and you should determine one internally, document it and STICK TO IT. Any lack of doing so will put you at risk.

- Be careful with people storing on their desktops though. They WILL look there without a shadow of doubt. A discovery process is not a fun one and you should have policies and procedures in place for whatever it is that you want to do. Documentation and standards are key

Challenges to compliance

- Changes to the I.T. environment
- Limited I.T. human resources
- Limited I.T. budget
- Cost to implement effective controls
- Compliance requirements are constantly changing.

Best practices for storing other types of records

- An email archiving policy should be part of an overall records management program, which has its own record retention policies and procedures.
- The scope of the policy should consider all employees who create, send or receive email messages and attachments.
- The email archiving policy should refer to IT's Acceptable Use Policy and expand upon the areas specifically related to email use.
- The policy should state whether users can create PST files to store email messages.
- Data privacy issues should be addressed. Employees should have no expectation of privacy when using company resources for email and could be subject to discovery proceedings and legal actions.

Best practices for storing other types of records

- The policy must clearly state how and where email records will be managed, protected and retained.
- The policy should explain how IT handles exceptions to the retention settings
- Managers and users must be provided with training and support.
- Compliance with the policy must be mandatory for all employees and include compliance in an internal audit review.
- Review the policy yearly to ensure compliance with any changes or new regulations.

How to stay compliant

- Adopt policies and standards that clearly state how long electronic records will be kept.
- Ensure that the organization sticks to polices by communicating requirements to employees.

How to stay compliant

- Monitor compliance by performing quarterly internal reviews.
- Monitor compliance by requiring annual external reviews by a third-party. This transfers risk from the organization and demonstrates due diligence.

How to stay compliant

- Do not make a practice of communicating policies to employees one time as part of the hiring process. Policies should be regularly communicated throughout all levels of the organization.

- Use the strengths and time of your I.T. personnel effectively and transfer high risk and high complexity systems to third parties such as Cloud and SAAS vendors.

How to stay compliant

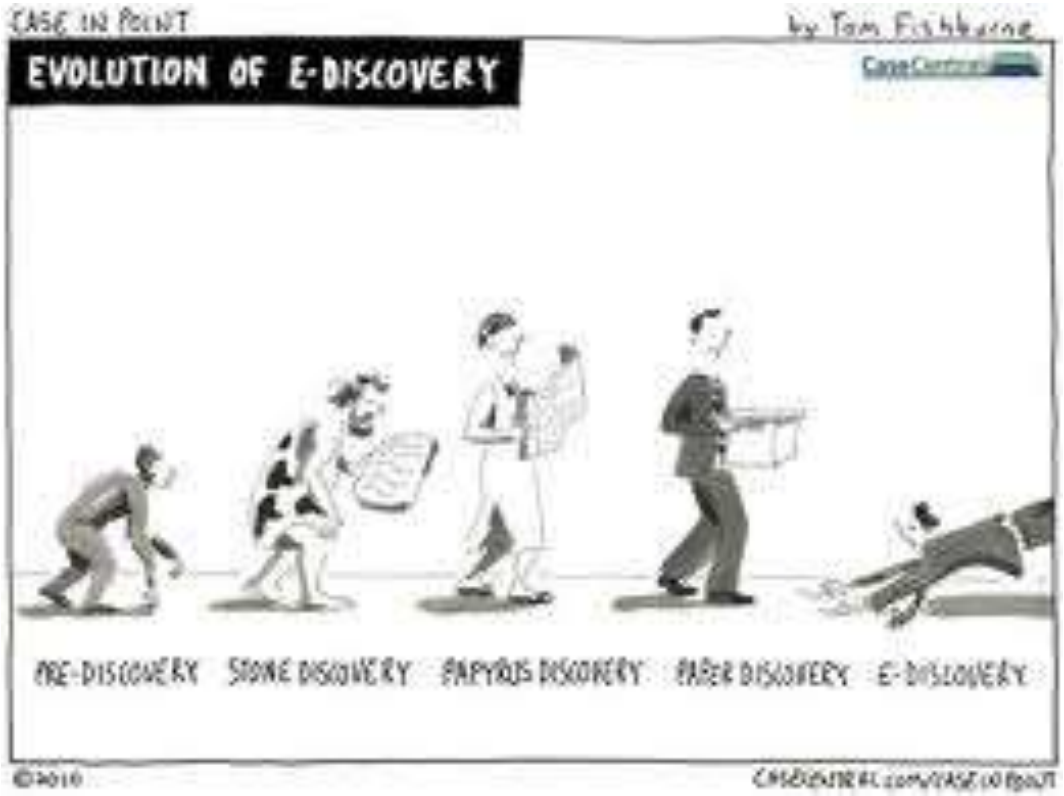
- Encourage continuing education for key positions in the organization.
- Management should review compliance status and make changes to policy as needed.

Responding to IT Security Incidents

- How prepared is your information technology (IT) department or administrator to handle security incidents? Many organizations learn how to respond to security incidents only after suffering attacks. By this time, incidents often become much more costly than needed. Proper incident response should be an integral part of your overall security policy and risk mitigation strategy.

- There are clearly direct benefits in responding to security incidents. However, there might also be indirect financial benefits. For example, your insurance company might offer discounts if you can demonstrate that your organization is able to quickly and cost-effectively handle attacks. Or, if you are a service provider, a formal incident response plan might help win business, because it shows that you take seriously the process of good information security.

Steps to Take



Steps to Take

1. Minimizing the Number and Severity of Security Incidents

- Clearly establish and enforce all policies and procedures
- Routinely assess vulnerabilities in your environment
- Establish security training programs for both IT staff and end users. The largest vulnerability in any system is the inexperienced user
- Routinely monitor and analyze network traffic and system performance
- Create a Computer Security Incident Response Team (CSIRT)

Steps to Take (cont.)

2. Assembling the Core Computer Security Incident Response Team

- The CSIRT is the focal point for dealing with computer security incidents in your environment. Your team should consist of a group of people with responsibilities for dealing with any security incident. Team members should have clearly defined duties to ensure that no area of your response is left uncovered.

- The ideal CSIRT membership and structure depends on the type of your organization and your risk management strategy. However, the CSIRT should generally form part or all of your organization's security team. Inside the core team are security professionals responsible for coordinating a response to any incident. The number of members in the CSIRT will typically depend on the size and complexity of your organization.

CSIRT

A successful CSIRT team consists of several key members.

- **CSIRT Team Leader.** The CSIRT must have an individual in charge of its activities
- **CSIRT Incident Lead.** designate one individual responsible for coordinating the response. The CSIRT Incident Lead has ownership of the particular incident or set of related security incidents
- **CSIRT Associate Members.** specific individuals who handle and respond to particular incidents. Associate members will come from a variety of different departments in your organization such **as Legal, PR, Management**

CSIRT

Activity	Role				
	CSIRT Incident Lead	IT Contact	Legal Representative	Communications Officer	Management
Initial Assessment	Owner	Advises	None	None	None
Initial Response	Owner	Implements	Updates	Updates	Updates
Collects Forensic Evidence	Implements	Advises	Owner	None	None
Implements Temporary Fix	Owner	Implements	Updates	Updates	Advises
Sends Communication	Advises	Advises	Advises	Implements	Owner
Check with Local Law Enforcement	Updates	Updates	Implements	Updates	Owner
Implements Permanent Fix	Owner	Implements	Updates	Updates	Updates
Determines Financial Impact on Business	Updates	Updates	Advises	Updates	Owner

Steps to Take (cont.)

- Make an initial assessment.
- Communicate the incident.
- Contain the damage and minimize the risk.
- Identify the type and severity of the compromise.
- Protect evidence.
- Notify external agencies if appropriate.
- Recover systems.
- Compile and organize incident documentation.
- Assess incident damage and cost.
- Review the response and update policies.

Storing electronic information while maintaining compliance.

ATA Technologies

www.atacpatech.net

Daniel Simons

Michael Laffoon