STATE ARCHIVING IN THE DIGITAL ERA

A Playbook for the Preservation of Electronic Records

October 2018

NASCIO
Representing Chief Information
Officers of the States

CoSA
Council of State Archivists

Introduction

The Council of State Archivists (CoSA) and the National Association of State Chief Information Officers (NASCIO) developed the following playbook for digital preservation of state electronic records. These national organizations and their members play a role in the development, management, reporting, preservation, and disposition of digital records. The following eleven plays should help both state Chief Information Officers (CIOs), state archivists, and other state leaders think about the best ways to preserve archives in this digital era.

Along with the successful execution of their digital strategies, current state CIO priorities focus on the effective and efficient delivery of digital services and reducing overall risk. Preserving state electronic records is a part of that risk management, and a necessary outcome of increasingly digital state governments.

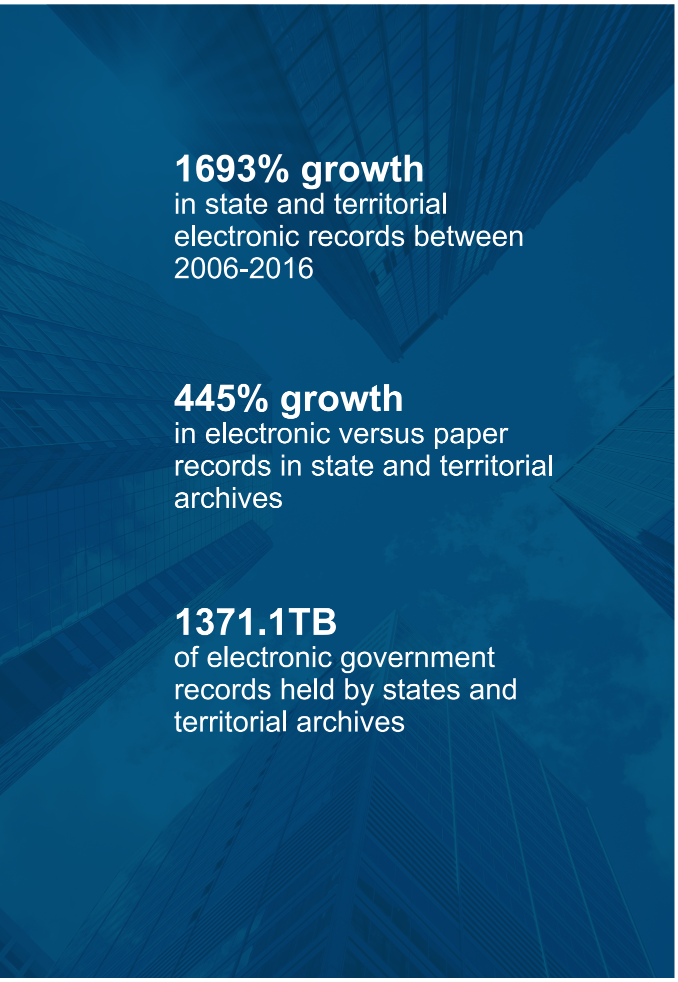
Digital preservation of state electronic records is a topic that touches upon and supports many of the top ten priorities of many state CIOs. Proper management of state electronic records mitigates information security risks by carefully managing personally identifiable information, managing legacy dependency, and ensuring state records are not locked in proprietary systems. State CIOs are deploying more cloud services and state enterprise-level efforts. Digital preservation services are frequently provided by third-party cloud providers or managed centrally by state agencies that provide service to others within the state.

The work that state CIOs are currently engaged in supports and directs the digital preservation of state electronic records. State archives and records management staff can help state CIOs apply their current efforts more effectively toward digital preservation by providing insight into state laws and statutes, and current practices. State CIOs can help reduce risk by ensuring that state electronic records are managed with optimized technology and that practices and policies are implemented at an enterprise level. Sound data management is also important to long term electronic records preservation.

Key Takeaways

1. There has been a dramatic and growing increase in the number of digital records in recent years.
2. States are not well prepared for long-term digital preservation.
3. The consequence is that electronic records are at risk and vulnerable.
4. State CIOs and State Archivists have key roles in the preservation of digital records.

Play 1.
UNDERSTAND THE NEED



1693% growth
in state and territorial electronic records between 2006-2016

445% growth
in electronic versus paper records in state and territorial archives

1371.1TB
of electronic government records held by states and territorial archives

State government is in the information business and data is its lifeblood. Public services create information in the form of records, increasingly in electronic formats. These records are essential to state governments and to the services state governments provide their citizens. States continue to struggle with new challenges presented by a growing portfolio of electronic records and digital content that must be preserved. The volume and complexity of electronic government records continues to increase at an exponential rate. When state government leaders work together, they can ensure the electronic records of today are available in the future to protect citizen rights, document government, and preserve history. Archives and records management staff can provide services to their state CIO as well as help them understand electronic records challenges.

Public records are public information (See Appendix A for definitions). Increasingly, government decisions and policies are being made and rolled out electronically. Most importantly, records are *key* to the documentation of government policies, actions and intent. Government data is often used at multiple levels of decision making. We need to capture and preserve these records.

Electronic records require attention to ensure they are preserved and accessible as they are more complex to preserve than paper records. Without action to preserve them, electronic records can be overwritten in databases, lost in media migrations, or become inaccessible due to incompatible legacy systems. Sustained attention and resources are needed to ensure the long-term management and accessibility of our nation's electronic records.

Play 2.
COLLABORATE FOR SUCCESS

E-records management is a cross-boundary group effort – a number of state agencies need to collaborate to ensure success. The increase in e-records and the explosion of digital content require governmental organizations to identify new strategies for properly managing electronic information. Collaborative effort is key to developing and adopting best practices and sustainable models for the long-term preservation of electronic records.

Joining stakeholder communities in a collaborative and holistic approach ensures that e-records are properly managed within the appropriate IT structure and archival requirements. The State CIO is a primary stakeholder with expertise in how electronic records management approaches and technologies fit within the state's strategic IT direction and enterprise architecture. State archivists and records managers are the primary stakeholders with expertise in which e-records to maintain, which to delete or deaccession, and what kind of access might be required. Other stakeholders may include: the Secretary of State's office, state legal counsel, the Attorney General's office, and state agency business unit and program owners.

Each stakeholder plays a different role in the management of electronic records.

- **State CIOs** have the experience to recommend technological solutions and services to better manage and preserve digital content.
- **Archives and records management staff** in your state provide critical expertise in navigating state statutes, traditions, and expectations.
- **Records managers** possess detailed knowledge about a state's records retention requirements and how they apply to electronic records.
- **State archivists** are responsible for records having historical or other significant value that necessitates permanent storage.
- **The state attorney general** and other state government lawyers have an interest in being able to readily locate and retrieve information requested during litigation and e-discovery. Their goal is to avoid legal liability for being unable to produce requested electronic documents. In addition, mechanisms and systems that facilitate easier searches through terabytes of electronic records can save legal counsel substantial amounts of time and state resources.
- **Individual agencies** must be able to contribute their perspectives with respect to electronic records management and how new initiatives might impact, and hopefully improve, their business processes, productivity, and compliance with records retention requirements.

The Oregon State Archives works to engage stakeholders early and continuously:

"The Oregon State Archives works closely with records creators throughout all levels of Oregon government. In the electronic environment this outreach has become ever more critical to engage more proactively and earlier in the lifecycle of the records. Our efforts are now focused on providing both the knowledge and tools necessary to ensure appropriate retention of and access to records. Our records management unit focuses on a unique statewide program whereby all public entities in Oregon, large and small, have the opportunity to gain access to complex electronic records management tools with the direct support and assistance of the State Archives. Without these early interventions it is a near certainty that many electronic records will become lost or inaccessible before their time. To date ORMS has facilitated the storage, and management, and disposition of over 5.5 TB of records." Kristopher Stenson, ORMS Administrator, Oregon State Archives

Play 3.
THE PITCH: COMMUNICATE PLANS AND EXPECTATIONS

Communicate to State Agencies

State agencies, offices, and employees must to adhere to public records laws. State CIOs work with many state agencies and have the ability to influence or direct policies and practices. It is important for agency employees, and possibly contractors, to understand their responsibilities around electronic records. Adequate employee awareness and training activities are keys to ensuring that employees correctly carry out new or existing policies and procedures and understand how to use any new technologies associated with improved electronic records management. This may include in-person or online training courses as well as ongoing follow-up and training to ensure that agency employees understand their part in ongoing records retention compliance. Training and awareness should include the following areas:

- An overview of the issues and challenges related to electronic records management in state government
- Records retention policies and schedules along with associated security, privacy and acceptable use policies
- Procedures for records retention
- Using any new technologies that have been implemented
- Understanding how records retention applies to alternative electronic communication devices (mobile devices, tablets) and methods, such as, instant messaging (Skype, Yammer, Vibe, Chatter), and whether text messages are considered records in your state
- Understanding how records retention applies to social media platforms such as Facebook, Twitter, Instagram, and others

Communicate to the State Legislature

State archivists and CIOs should be prepared to explain to the state legislature the challenges associated with the dramatic growth in electronic records. State legislatures can support the preservation of essential state electronic records by supporting and funding electronic records programs and passing legislation and statutes to support electronic records management and long-term digital preservation.

Communicate with the Public

Electronic records touch the public at all the significant points in life: vital statistics record birth and death; courts record marriages, divorces, deeds, and trusts. The public needs to be confident that the security, confidentiality, and integrity of those records are maintained. Personally identifiable information can also appear in public comments on government social media platforms. It is helpful to have a clearly publicized policy on how state government agencies handle this information. State archives staff can help agencies develop the appropriate policies.

Play 4. KEEP PUBLIC BUSINESS ON PUBLIC PLATFORMS

State CIOs are often asked to acquire, configure and deploy communication platforms to support state business. **It's important to emphasize that any account that is used for state business is subject to public records laws.** The accounts must be managed and archived according to public records laws. If personal social media accounts are used for government business, the content created is nevertheless a public record.

To simplify compliance, be sure that all public officials use official media accounts for state business. Personal accounts should be used for personal communication. Personal communications should not be made via public accounts. Likewise, it is best practice for campaign accounts and public accounts to be separate and used only for their intended purposes.

Official accounts should be used for all government business that happens via social media. Personal accounts can be used to amplify government account communications, however, official government communications should not originate from a personal account. State business should occur on state accounts.

Keeping public records on public accounts simplifies the management and preservation of e-records, limits costly legal battles over public records, and makes long-term access of state electronic records much simpler.

Play 5. MANAGE EMAIL RECORDS

Email is one of the most important electronic communication tools in the workplace, including in state government business. Identifying emails that are permanent or long-term electronic records within an email account and properly managing them for long-term use is an important responsibility (see Appendix B for guidance on email management and a checklist for managing email). Email messages are subject to public records laws and statutes and need to be managed accordingly. There are many instances in which email may contain state electronic records including:

- Documents and work processes routinely circulated via email
- Appointments to boards and commissions
- Hiring and firing decisions
- Instructions given to and reports from cabinet and agency officials
- Contract negotiations
- Legal and policy decisions

Play 6.
LEGACY DATA AND DATA MANAGEMENT

Electronic records are more complex to preserve than paper records and they require regular attention. They also need to have appropriate technology in place to facilitate their management and storage. Most state agencies will need to simply develop a plan to identify and transfer public records to the appropriate agencies on a regular and ongoing basis.

Fast-Moving Technology:
Technological obsolescence is a primary issue for states in determining what types of solutions or technologies to choose. The concern stems from the fact that technology is evolving at an accelerating rate. This means that, for example, the hardware and software many agencies use today will likely be obsolete in a few years. These concerns are magnified in the e-records context in the following ways:

- The file formats of e-records may change and become unreadable even by subsequent releases of the software that created them.
- Electronic objects require special monitoring to maintain the evidentiary status of the records. Establishing fixity, or the property of a digital file or object being fixed or unchanged, is a critical part of confirming evidentiary status of electronic records. The PREMIS data dictionary defines fixity information as "information used to verify whether an object has been altered in an undocumented or unauthorized way." Fixity can be established via checksums or cryptographic hashes and is frequently relied upon to provide proof of the electronic record's reliability and authenticity. It is necessary to collect and preserve fixity information throughout the lifecycle of the state electronic record.
- Some systems for document management don't preserve the content, structure, context and integrity of the record over time.

States must select technologies that properly manage and store electronic records, while ensuring that the inevitable obsolescence of the technology does not compromise the records' integrity or accessibility.

Enterprise Electronic Storage Options:
During an e-records initiative, states may consider solutions for the enterprise that can be used by multiple agencies. Typical categories of solutions include:

- Electronic Records Management System (ERMS): Manages records from their creation to final disposition, including categorizing and locating them.
- Electronic Content Management System (ECMS): Organizes, controls and facilitates the publication of a large body of documents, including versioning and track changes.
- Electronic Document Management System (EDMS): Facilitates the creation of a document and allows for storing, editing, printing and other processes. It usually provides a single view of multiple databases.

Within the context of some e-records initiatives, some states may examine whether to adopt a standard file format to be used on an enterprise basis. In examining this issue, important considerations center upon technology obsolescence in a quickly changing technology environment. Backwards compatibility issues also have been part of this conversation in terms of gauging the impact on agencies that are unable to purchase software to comply with a standard file format.

Play 7.
CHANGING OPERATING MODELS

The roles of State CIOs have been evolving. In addition to being owner-operators of state IT systems, they are increasingly managing third-party service providers. State CIOs are brokers with multisourcing service contracts such as those for email, which is frequently an enterprise level service and often outsourced. Likewise, digital preservation of electronic state records is also undergoing changing operating models.

State archives and records management staff are performing digital preservation in-house and outsourcing preservation services. One example is Archive-It, a subscription-based web archiving service from the Internet Archive, that helps organizations harvest, build, and preserve collections of digital web content. Using the service's web application, state archives can collect, catalog, and manage their collections of archived web content. The subscription service can provide 24/7 access. Content is hosted and stored at the Internet Archive data centers and can be sent to state archives as well. Another digital preservation service that is a solution provider in state government electronic records is Preservica. Preservica currently provides digital preservation services to 19 US state archives and offers both cloud-hosted (SaaS) and on-premise digital preservation software. The service can also provide user access to electronic records through a user interface based on Wordpress.

No matter the preservation service provider, the service agreement needs to be thoughtfully and carefully developed. An exit strategy should be identified as part of the contract. The need for digital preservation of state electronic records will outlast commercial service providers and current technological infrastructures. The state needs to clearly understand its rights regarding its data and how the preservation provider is helping it perform its obligations to its citizens.

Contract Issues to Watch for

- What are the costs of retrieving data required for access or transfer?
- Do the vendor's financial models match those of your state?
- How is changing technology impacting your vendor?
- How will you get your data if your vendor ceases operation?

In addition to home-grown preservation services and traditional fee-for-service providers, state archives are also engaging in community-based preservation tools such as BitCurator. The BitCurator Consortium supports the ongoing maintenance and software development of the BitCurator project. The project's digital forensics software tools incorporate archives workflows and helps to eventually provide public access to the data. The project initially began developing the software tools in 2011 and has developed training modules, provided ongoing maintenance to the software, and made improvements over the years. BitCurator's support by the preservation community ensures that the software continues to be properly supported for archives and library users.

As the roles of state archives expand, state CIOs can provide valuable insights into how archives can mitigate outsourcing risks and how best to manage a variety of operating models.

Play 8.
SECURITY AND RISK MANAGEMENT

Security and risk management are critical topics for digital preservation of state electronic records. State archives have to protect data themselves while simultaneously ensuring that third-party service providers are properly protecting data (see Appendix C, “Digital Preservation Coalition Checklist: questions for your preservation storage service provider.” While digital preservation capability is maturing in all states along all of the fifteen points of the Digital Preservation Capability Maturity Model, state archives continue to face data security issues. As states are engaging more managed services and outsourcing more digital preservation activities, the states have to be confident that third-party security practices are keeping electronic state records secure. While contracts can be formulated to guarantee security arrangements required by state laws and statutes concerning public records, in the real world data remains vulnerable to hacks and hostage situations regardless of contract provisions. State institutions may decide that having limited control over sensitive data is a risk worth taking to have third-party providers handle digital preservation lifecycle services, but it needs to be an informed decision. State CIOs can help state archives and records management personnel perform a cost-benefit analysis about outsourcing preservation services in relation to data security.

Contracts with third-party digital preservation service providers should establish responsibility for functions that are critical to ensuring the integrity of state data including fixity checking and audits or compliance with state government legal responsibilities. Audit trails are also important to establish when working with a third-party preservation service provider. A verifiable audit trail of the activities involved in the processing of digital records ensures that the reliability and authenticity of the data is secure.

In addition, NASCIO recommends that states adopt a data classification policy. This helps secure data by knowing what data is most sensitive and most in need of higher levels of security.

In the summer of 2018 *the Minnesota State Archives as well as those from many other states were sent letters and compact discs purporting to contain a deposit: a database of artificial intelligence software. The letter claimed the data is closed to the public but has no copyright and must be cleared for access by contacting the Chinese Embassy. The Minnesota State Archives personnel had enough security training to pick up on the questionable elements of the deposit. They reached out to get help and avoided compromising their systems. In cases of questionable deposit, the state information security officer or the state CIO’s office is usually the next contact for a state archives office and can help the state archives, records management personnel and law enforcement take the appropriate next steps.*

Play 9.
IDENTIFY RECORDS; DELETE NON-RECORDS

It is critical to preserve e-records for the appropriate amount of time as specified under state law or statute and in records retention schedules and policies. State archives and records management personnel can help determine which electronic files qualify as electronic records. The role of records retention laws and schedules is to assist state agencies in taking intellectual control over their e-records by being able to determine what information qualifies as a record and how long records should be kept. While laws vary from state-to-state, a record normally is a piece of information that documents an organization's "functions, policies, decisions, procedures, operations" or other significant activities. From there, decisions can be made about whether a record can be made publicly available or produced in the event of an open records or Freedom of Information Act request. Disposing of non-records when appropriate minimizes the amount of data that needs to be stored. When the records management schedule indicates that it is ok to dispose of or delete electronic records, do so in compliance with retention policies.

Dash camera footage, body camera footage, and other digital video or audio recordings have the potential to be public records and can influence court decisions. These large files are also created daily as part of the work of law enforcement officers. While these videos can provide important evidence, they can also overwhelm systems if not properly managed. States are in the process of developing and implementing records schedules or retention policies for these kinds of digital video content. As with many issues, state requirements vary from state to state (see Appendix D for examples of different state retention requirements for body and dashboard cameras).

Play 10.
IMPLEMENT SOCIAL MEDIA POLICIES AND STANDARDS

Social media are an important and pervasive part of modern life. Facebook, Twitter, Instagram, and other social media are where people go to get significant and timely information -- including government information. Significant governance is happening via social media. Social media communications have been used in court cases and to calm the public in times of uncertainty. Public policy is unveiled on Twitter. Instagram and Facebook are offering insights into government decisions and practices. As a result, social media content and accounts are required to be preserved as public records (see Appendix E for a checklist for using social media in government). State archives and records management personnel can help determine which records have long-term value and how to preserve them. Records in social media that should be captured and preserved may include:

- Evidence of an administration's policies, business, or mission
- Information only available on the social media site
- Official agency information
- Direct communication with the public using social media

Play 11.
THE TOUGHEST PLAY: DEDICATE FUNDING

Ongoing resources are needed to ensure the long-term management and accessibility of state electronic records. Sustained funding and increased investment in collaborative research are key to identifying best practices and models for the long-term preservation of electronic records.

To assist states with considering innovative ways to fund technology initiatives, NASCIO previously completed research that identified and described innovative state IT funding and financing models that were successful in the states. Many of these models may be applicable to electronic records management and digital preservation projects. Options include:

- Benefits funding (funding through benefits realized by project implementation)
- Bonds
- Budget and appropriation strategies
- Fee-for-service revenue
- Investment funds
- Outsourcing and managed services
- Performance-based contracting
- Public-private partnerships
- Purchasing and procurement strategies
- Sharing services
- Grants

States and territories spend on average **.007%** of the amount of the total annual budget on all archives and records management functions, including preservation of electronic records.

LOOKING FORWARD

As states pursue efforts to improve electronic records management, they must consider the key benefits. With a formal electronic records management strategy and execution, state agencies benefit from more organized electronic records because information is more readily available and accessible to policy makers, public records requests and collaborative initiatives. Additionally, e-records management projects provide an opportunity for agencies to simplify and streamline their back-office activities.

Traditionally, the focus of many electronic records management initiatives has been internal, particularly for those records with fiscal and accounting value, such as agency financial transactions and obligations. With the emerging theme of greater state government transparency and accountability, these records now have an external-facing value. It is obvious that easy discovery, presentation, and access to fiscal electronic records will continue to grow as an expectation by the public.

Improving electronic records management across the state enterprise will lead to a substantial reduction of risk and liability. With more information existing in electronic form, states face the risk that information will be lost or not retrievable in the event of a lawsuit. If e-discovery record searches result in an inability to produce requested records, the state could face penalties, adverse jury instructions at trial, or even the loss of a court case. However, an enterprise approach to managing electronic records can ensure that records are:

- Appropriately identified
- Properly classified
- Maintained according to records retention policies
- Stored in a way that makes them easily locatable and retrievable
- Effectively preserved or destroyed according to retention policy and schedules
- Addressed in the state’s emergency response plan and adequately protected during a disaster

Improved electronic records management can also reduce legal risk associated with non-compliance with state or federal laws and regulations.

For state CIOs, a focus on this universal business problem offers a shared services opportunity: an enterprise electronic records storage, management, and digital archival environment shared by agencies. With a shared services model, the potential risks associated with non-integrated, proprietary or standalone systems can be avoided. This will save states substantially by precluding each agency’s attempt to create and fund its own solution.

The dramatic and accelerating increase of electronic records certainly presents challenges for states that are not prepared. However, by working together, taking an enterprise vision and communicating to key players, state archivists and state CIOs can begin to set in motion a plan to preserve digital archives for the future.

APPENDIX A

Definitions

i) **E-Records**: A “record” is the term used to describe a document, regardless of format, that is evidence of conducting state business. For example, a record may memorialize a transaction conducted by the state. In this brief, an “e-record” or an “electronic record” is a government record that is in digital form, which could range from email to word processing documents to digital images.

ii) **E-Records Management**: Electronic records management is an approach to organizing electronic government records so that they are locatable, retrievable, and stored in accordance with state records retention schedules. This also includes the timely deletion or destruction of e- records after the expiration of retention time periods, unless extenuating circumstances such as litigation require otherwise.

iii) **Digital Preservation**: Digital preservation combines policies, strategies and actions to ensure access to reformatted and born digital content. The goal of digital preservation is the accurate rendering of authenticated content over time. State electronic records require digital preservation. Some state records have short term retention needs, but there are many government documents that have significant value and must be retained permanently. State archivists normally oversee which records are encompassed within this category and ensure the preservation of those records.

APPENDIX B

Guidance on Email Management

The bulk of email may not need to be preserved because of its transitory nature, but the content of the email will determine how long an email record is retained. However, a notable exception would be legal counsel’s email. Since standards exist for addressing the retention of emails, state archives and records management staff can clarify state policies, standards, and practices regarding retention and preservation of email records. Email systems may have auto-archive and delete functions that should be turned off to avoid any interference with state records retention schedule compliance. Auto-delete functions may necessitate that employees classify their emails before a specified time period elapses, such as 90 days, after which an email will be deleted. Emails may be classified and stored in folders of similar content or retention period—this should be done when an email is received to avoid conducting this process for hundreds of emails at a time. State agencies have a responsibility to follow policy and train new users on effective email management. State archives and records management personnel can assist you in determining whether these features will comply with your state records retention and disposition requirements. Agencies have a responsibility to develop policy and to train users on how to properly handle their email.

Increased use of email has led to issues of how to store emails that must be retained for varying lengths of time. Many state CIOs are facing this issue in the context of the trend towards greater consolidation and use of cloud solutions for state email systems. Instead of storing all emails within employees’ email in-boxes, states should opt for policies and solutions to store email in a systematic way outside of the employee’s in-box. The benefits of this approach range from overall cost reductions to reducing storage space required for non-critical emails. Options for storing archived emails range from the creation of an email archive, to storage on hard drives and peripheral devices, to cloud storage.

Large organizations realize e-discovery can be burdensome. In states where email is an enterprise shared service, state CIOs should be prepared for frequent requests from their agency customers for access to copies of email and text messages or prepare the agencies to handle their own access requirements. With the migration to enterprise cloud-based email and depending on business model and platform, state agencies remain the custodians of employee email. The agencies may consider distributed e-discovery capabilities for agency legal staff preferable to requests to the CIO office. Request for access to emails can be costly in terms of staff time as the email files typically need to be reviewed to determine if the content is protected from or subject to public disclosure. Having a clear policy in place and consistently applying it can ensure that the emails that are e-records are properly managed and others are properly disposed of in accordance with state records retention policies.

Checklist for Managing Email

- States need to manage the content of email records, not the servers or platforms on which the messages are stored.
- Ensure that staff members are aware of the extent to which their email and text messaging is a public record and may be disclosed publicly.
- Establish clear policies relating to the use of email and text messaging, including limits relating to personal communications and nongovernmental business transactions.
- Seek guidance from your state archives or records management agency and develop appropriate records retention policies and disposition schedules to be used for email and text messages.
- Seek expert legal advice regarding your state laws on the retention and public access to email, text messages, and any other electronic communication records. This includes communications generated during transitions into and out of office, and communications using private email, cell phones, or any electronic communication relating to public business.
- Establish policies regarding the use of personal email accounts to conduct official business. In many states, public records laws and/or legal precedents define any message, regardless of originating/receiving account, that concerns public business as a public record subject to public discovery and other requirements.
- Be prepared for frequent requests for access to copies of email and text messages and be prepared to invest the staff resources needed to review large volumes of email to determine whether it is protected from or subject to public disclosure.

APPENDIX C

Digital Preservation Coalition Checklist: questions for your preservation storage service provider

- What level of redundancy does the storage system provide? How many physical locations is digital material held in? What is the geographical distance between them?
- Are different types of storage technology employed to mitigate/ spread risk? For example, online and off-line storage.
- If a file has become corrupted or unintentionally altered, how does this get detected and when does detection happen? Are audit trails or other forms of logging available to show that data integrity checks have been done and to show the result?
- What is the disaster recovery strategy, for example if a storage system fails or there is a natural disaster at a storage site then how are digital materials recovered? When was the last time this DR strategy was tested?
- What is the storage migration strategy to address technical obsolescence? What happens when the system is at the end of its life and content needs to be migrated to a new system? Is the content still accessible during this process?
- What is the exit strategy when using a given type of storage (e.g. onsite, cloud) for example what happens if the vendor of the storage system goes out of business?
- What measures are in place to contain corrupted or altered files, for example quarantining files to prevent them from being replicated?
- What security and auditing measures are in place to prevent unwanted access and/or modification of the digital materials?
- Who is responsible for monitoring and managing the storage system to ensure it is functioning correctly? Is there continuity of staff in cases of holiday, sickness or departures?
- What contracts, warranties or guarantees come with the storage solution or service that commit the vendor or supplier to support, recover or replace if there are any problems?
- What approach or support is in place for storage technology watch and risk assessment so that migrations, refreshes, upgrades or maintenance can be planned and executed in a timely way?
- Are the costs and risks clear so that a trade-off can be assessed and made between number of copies, type of storage, ease of access, and safety of the digital materials?
- What standards does the provider aim to comply with? (e.g. OAIS, Information Security Standards) Does it aim to achieve recognition as a trusted digital repository?
- How can the provider demonstrate they are doing what you have agreed?

APPENDIX D

Examples of different state retention requirements for body and dashboard cameras:

Florida	Retention 90 days
Utah	After resolution of issue, then destroy records.
Georgia	30 months if video is part of an investigation, vehicular accident, shows an arrest, use of force or can be anticipated for use in pending litigation
North Carolina	RETAIN UNTIL: Complete PLUS: 30 days THEN: Destroy NOTE: Records that become part of a case file should be handled according to those disposition instructions.
Kentucky	Retain all recordings of DUI-related incidents for fourteen (14) months if there is no appeal or if they do not document the actual happening of an accident involving a motor vehicle or after a decision has been made not to prosecute. Destroy upon order from District Court. If the actual happening of an accident is recorded, retain twenty-six (26) months if there is no appeal. Destroy upon order from District Court. Retain non-evidentiary recordings for thirty (30) days, then destroy. Evidentiary recordings used in any investigation, pending investigation, litigation or open records requests must be kept until all investigative or legal activity is completed. Then destroy the original and all copies of the recording.

Consult with state archives and records management personnel to determine the most up-to-date retention practices within your state.

About NASCIO

Founded in 1969, the National Association of State Chief Information Officers (NASCIO) represents state chief information officers (CIOs) and information technology (IT) executives and managers from the states, territories and District of Columbia. NASCIO's mission is to foster government excellence through quality business practices, information management and technology policy. NASCIO provides state CIOs and state members with products and services designed to support the challenging role of the state CIO, stimulate the exchange of information and promote the adoption of IT best practices and innovations. From national conferences to peer networking, research and publications, briefings and government affairs, NASCIO is the premier network and resource for state CIOs. For more information, visit www.NASCIO.org.

About CoSA

The Council of State Archivists (CoSA) is a nonprofit membership organization of the state and territorial government archives in the fifty states, five territories, and District of Columbia. Through collaborative research, education, and advocacy, CoSA provides leadership that strengthens and supports state and territorial archives in their work to preserve and provide access to government records. CoSA facilitates networking, information sharing, and project collaboration among its member organizations to help state and territorial government archives with their responsibilities for protecting the rights and historical documents of the American people.

APPENDIX E

Checklist for Using Social Media in Government

- □ Develop a social media policy
- □ Review terms of service agreements for social media
- □ If permitted by the terms of service, maintain official accounts for official information
    - ○ Only use official government social media accounts for official business (keep personal information on personal accounts)
    - ○ Use campaign accounts for campaigning and official accounts for official business
- □ Understand that social media is a public record
    - ○ Develop a records retention policy and regularly transfer social media records to the appropriate agencies, such as your state archives
    - ○ Hand off social media accounts from one administration to the next to maintain consistency and integrity
    - ○ Comments or messages on social media platforms may also be subject to public record laws. As public records, these comments and messages would also be subject to any laws requiring the redaction or removal of sensitive or personally identifiable information.

AUTHORS

Michelle Gallinger
State Electronic Records Initiative (SERI) Coordinator, CoSA

Amy Hille Glasscock
Senior Policy Analyst, NASCIO

Doug Robinson
Executive Director, NASCIO

CONTACTS

CoSA
Michelle Gallinger or Barbara Teague, 502.229.8222
info@statearchivists.org

NASCIO
Amy Hille Glasscock
859.514.9148
aglasscock@NASCIO.org

Support for this publication was provided by the Institute of Museum and Library Services (IMLS) through a National Leadership Grant to the Council of State Archivists (CoSA) for Archives Collaborating and Cooperating with External Strategic Stakeholders (ACCESS), a project of the State Electronic Records Initiative (SERI).

NASCIO Representing Chief Information Officers of the States

CoSA Council of State Archivists