Fall 2014

Protection of Personal Information

Security and Incident Investigation Procedures and Practices for Local Governmental Units

Effective January 1, 2015

Darren T. Sammons, Staff Attorney
Commonwealth of Kentucky
Fall 2014

Introduction

Definitions:

"*Computer security incident*" or "*incident*" means a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.[1]

"*COT*" means the Commonwealth Office of Technology.[2]

"*Digital media*" means physical, electronic media, used to store information, including, but not limited to: diskettes, magnetic tapes, desktop computers, laptops, hard drives, random access memory, read only memory, compact discs, network equipment, other forms of optical and magnetic media, and any other electronic media on which information may be stored. This definition includes forms of media existing at the time these regulations are promulgated and also any such forms or formats as may be invented.

"*DLG*" means the Department for Local Government.[3]

"*Local Governmental Unit*," or "*LGU*" means every group, governmental entity and governmental subdivision identified by KRS 61.931(1)(b) and (c) that are not organizational units of the executive branch of state government of the Commonwealth of Kentucky.[4]

"*Non-digital media*" means a hard copy or physical representation of information, including, but not limited to, paper copies, printer ribbons, drums, microfilm, platens, and other forms of preserved or preservable information.

"*Portable computing device*" means electronic devices on which personal information is stored, or may be stored, designed, used or intended to be used in multiple physical locations or capable of being used while traveling, such as laptops, tablet computers, personal digital assistants (PDAs), digital cameras, portable telephones, and similar devices.

For purposes of this policy, all terms not otherwise defined are used consistent with the definitions set forth in KRS 61.932.

Policy Statement: The purpose of this policy is to provide guidance to Local Governmental Units ("LGUs") to minimize the risk of disclosing personal information and setting practical guidelines for effectively responding to security incidents. LGUs are encouraged to tailor this policy to meet their own specific security and operational requirements. Having a policy is important because it promotes consistent response procedures to make sure appropriate actions are taken. This policy sets forth the procedures and practices pursuant to KRS 61.932 for LGUs to follow in order to:

1) Identify vulnerabilities;
2) Eliminate or mitigate those vulnerabilities;
3) Recognize when an incident has occurred;
4) Notify appropriate personnel in the event of an incident;
5) Respond to information security threats; and
6) Recognize events that require special handling due to their potential impact or special reporting due to legal or other concerns.

In addition, this policy requires LGUs to enact appropriate measures to protect information stored on media, both digital and non-digital, during the entire term of its use, until its destruction.

Policy Maintenance: The Department for Local Government ("DLG") will be responsible for maintaining this policy. LGUs may adopt this policy or may elect to adopt more restrictive policies as appropriate.

Applicability: In the absence of more restrictive policies, this policy shall be followed by all LGUs with access to personal information and also by any and all persons or entities with access to such information in the possession or control of LGUs. Such persons or entities include, but are not limited to, employees, contractors, consultants, temporary employees, volunteers and other workers with access to personal information whether printed, electronic or other format.

Responsibility for Compliance: Each LGU is responsible for ensuring that employees and others with permissive access to, or who may access, personal information are familiar with the policy and all such persons or entities shall be aware of what constitutes an incident. Each LGU shall ensure that employees are aware that compliance with this policy is mandatory. LGUs have the responsibility to enforce this policy.

Policy

Non-digital media containing personal information shall be physically controlled and securely stored in a manner meant to ensure that the media cannot be accessed by unauthorized individuals. This may require storing media in locked containers such as cabinets, drawers, rooms, or similar locations if unauthorized individuals have unescorted access to areas where personal information is stored. If personal information is stored in an electronic format, it shall be protected from access by unauthorized individuals. Such information must be protected by software that prevents unauthorized access. If personal information is transmitted via e-mail or other electronic means, it must be sent using appropriate encryption mechanisms.

Point of Contact

Every LGU shall designate a Point of Contact ("POC"). The POC shall serve the following functions:

1) Maintain the LGU's adopted Information Security Policy and be familiar with its requirements;
2) Ensure the LGU's employees and others with access to personal information are aware of and understand the Information Security Policy;
3) Serve as contact for inquiries from other agencies regarding its Information Security Policy and any incidents;
4) Be responsible for ensuring compliance with the Information Security Policy; and
5) Be responsible for responding to any incidents.

_____

Software

Security software used to protect personal information must provide user identification, authentication, data access controls, integrity, and audit controls.

Security software should be adequately tested to confirm functionality and to ensure that it is minimally disruptive to all associated operating systems, communications, applications, and other associated software systems. Contractual provisions must also ensure that the supplier's software, by design or configuration, will not introduce any security exposures.

The level of protection afforded by security software should be commensurate with the sensitivity of the data. For example, if data resides in a database that is deemed highly confidential, stringent access controls to the database should be employed. The level of protection along with the methods to implement that protection should be addressed before any personal information is stored on a device.

Systems, networks and application software used to process personal information must adhere to the highest level of protection reasonably practical. LGUs shall use Intrusion Detection and Prevention software approved by COT. A list of approved software is available on the COT website.[5] As an alternative, LGUs may use software not approved by COT, provided that such software provides comparable, or superior, protection.

Encryption

Information stored on digital media shall be encrypted in accordance with contemporary standards.

Access Control

Only authorized individuals are permitted access to media containing personal information. In addition to controlling physical access, user authentication should provide audit access information. Any access must comply with applicable regulatory requirements.

Portable Computing Devices

This policy prohibits the unnecessary placement (download or input) of personal information on portable computing devices. However, users who in the course of LGU business must place personal information on portable computing devices must be made aware of the risks involved and impact to the affected person/entities in the event of actual or suspected loss or disclosure of personal information. If personal information is placed on a portable computing device, reasonable efforts must be taken, including physical controls and encryption, to protect the information from unauthorized access. Additionally, each person using the portable computing device must sign a form approved by the LGU indicating acceptance of the information and acknowledging his/her understanding of the responsibility to protect the information. In the event the portable computing device is lost or stolen, the LGU should be able to accurately recreate the personal information and must be able to provide notification to all affected persons/entities.

When it is determined that personal information must be placed on a portable computing device, every effort should be taken to minimize the amount of information required. If possible, information should be abbreviated to limit exposure (e.g., last 4 digits of the social security number).

Physical Security Procedures

Given the broad variety of sizes and types of LGUs, each will have different security challenges and resources available to address those challenges. This policy does not specifically address physical security needs and threats, such as natural disasters, electrical outages, fire, or other physical threats to personnel or information resources. LGUs are responsible for establishing and maintaining their own physical security procedures.

The Information Security Policy adopted by an LGU shall include provisions calculated to ensure that its information resources are protected by physical security measures that address physical tampering, damage, theft, or unauthorized physical access. Where applicable, the Information Security Policy should address the circumstances under which identification badges must be worn and establish parameters for access to restricted areas containing information technology resources or other sources of personal information.

When feasible, information technology equipment should be marked with some form of identification that clearly indicates it is the property of the LGU. During transport, media shall be protected and controlled outside of secured areas and activities associated with transport of such media restricted to authorized personnel. Tracking methods shall be developed and deployed to ensure media reaches its intended destination.

Protection of Personal Information

LGUs shall secure and, when applicable, appropriately dispose of non-digital media. Non-digital media containing personal information must be properly stored and secured from view by unauthorized persons.

Secure measures must be employed by the LGU and all permissive users to safeguard personal information contained on all LGU technology resources.

LGUs shall ensure that all authorized personnel are familiar with and comply with the Information Security Policy. LGUs shall ensure that only authorized personnel may hold and have access to personal information.

Types of Incidents

Threats to the security of personal information arise in many different ways. LGUs are encouraged to be aware of the different types of threats and to enact reasonable measures to protect against each. Attacks on personal information may arise from:[6]

- External/Removable Media—an attack executed from removable media (e.g. flash drive, CD) or a peripheral device.
- Attrition—An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.
- Web—An attack executed from a website or web-based application.
- Email—An attack executed via an email message or attachment.
- Improper usage—Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.
- Loss or Theft of Equipment—The loss or theft of a computing device or media used by the organization, such as a laptop or smartphone.
- Other—an attack that does not fit into any of the other categories.

Destruction of Records Containing Personal Information

A media retention schedule shall be defined for all media in accordance with regulatory requirements. LGUs are encouraged to adopt a retention schedule consistent with the Kentucky Department of Libraries and Archives General Records Retention Schedule for State Agencies.[7]

Every LGU shall have a document/information retention policy. When records containing personal or confidential information are ready for destruction, LGUs shall destroy the information completely to ensure that the information cannot be recognized or reconstructed. In addition, any personal or confidential data contained on the computer media must be obliterated and/or made indecipherable before disposing of the tape, diskette, CD-ROM, zip disk, or other type of medium.

Each LGU must provide appropriate methods and equipment to routinely destroy personal or confidential information. The methods set forth below are listed in priority order with the most highly recommended safeguard listed first. One of the following safeguards must be implemented:

- Hire a document disposal contractor to dispose of the material. The contractor should be certified by a recognized trade association and should use disk sanitizing software and/or equipment approved by the United States Department of Defense. The LGU should review and evaluate the disposal company's information security policies and procedures. The LGU should review an independent audit of a disposal company's operations and/or its compliance with nationally recognized standards.
- Secure and utilize shredding equipment that performs cross-cut or confetti patterns.
- Secure and utilize disk sanitizing or erasing software or equipment approved by the United States Department of Defense.
- Modify the information to make it unreadable, unusable or indecipherable through any means

---

Reporting of Incidents Involving Personal Information

Each LGU must disclose a security breach in which personal information is disclosed to, or obtained by, an unauthorized person. Notification of the incident must be made in the most prompt and expedient manner after the incident has been discovered. Within thirty-five days, a letter notifying affected individuals of actual or suspected loss or disclosure of personal information must be sent by the LGU describing the types of information lost and recommended actions to be taken to mitigate the potential misuse of their information.

When a LGU identifies that a security breach has occurred in which personal information has been disclosed to, or obtained by, an unauthorized person, within three business days it shall notify Kentucky State Police, the Auditor of Public Accounts, the Attorney General and the Commissioner of the Department for Local Government[8] and complete form COT-F012. The LGU shall document the following:

1) Preliminary Reporting and description of the incident;
2) Response, including evidence gathered;
3) Final Assessment and corrective action taken; and
4) Final Reporting

Incident Response procedures can be a reaction to security activities such as:

1) Unauthorized access to Personnel, Data, or Resources;
2) Denial of Service Attacks;
3) Actual or Anticipated Widespread Malware Infections;
4) Data Breaches;
5) Loss/Theft of Equipment;
6) Significant Disruption of Services
7) Significant Level of Unauthorized Scanning Activity to or from Hosts on the Network

---

Investigation: LGUs shall make reasonable efforts to investigate any security breaches in which personal information is disclosed to, or obtained by, an unauthorized person and shall take appropriate corrective action.

Disclosure Communications: LGUs must comply with all federal and state laws and policies for information disclosure to media or the public. In some circumstances, communication about an incident is necessary, such as contacting law enforcement. LGUs should use discretion in disclosing information about an incident. Such information includes network information, type of incident, specific infection type (if applicable), number of assets affected, specific detail about applications affected, applications used to employ corrective action/investigate, etc. LGUs may proactively share relevant incident indicator information with peers to improve detection and analysis of incidents. Within the parameters of the law, minimal disclosure regarding incidents is preferred to prevent unauthorized persons from acquiring sensitive information regarding the incident, security protocols and similar matters, in an effort to avoid additional disruption and financial loss.[9]

References

[1] "Computer Security Incident Handling Guide," National Institute of Standards and Technology, U.S. Department of Commerce, p. 6; http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

[2] KRS 42.724

[3] KRS 12.023(3); 147A.002, et seq.

[4] http://www.lrc.ky.gov/Statutes/statute.aspx?id=43575

[5] https://gotsource.ky.gov/docushare/dsweb/Get/Document-301110/

[6] "Computer Security Incident Handling Guide," National Institute of Standards and Technology, U.S. Department of Commerce, p. 2.

[7] http://kdla.ky.gov/records/recretentionschedules/Documents/State%20Records%20Schedules/kystateagency.pdf

[8] KRS 61.933(1)(a)1.

[9] "Computer Security Incident Handling Guide," National Institute of Standards and Technology, U.S. Department of Commerce, p. 9.