

State of Iowa
Iowa Lottery Authority

Data Classification and Handling Procedures

Standard

Effective June 1, 2007

Iowa Lottery Authority
DATA CLASSIFICATION STANDARD

IDENTIFICATION

This standard establishes the criteria for classifying data and information into three categories of confidential, sensitive, and public. This classification applies to the data only and not to the tool which eventually displays the information. As an example, Outlook is a tool that reads an email file and displays the data onto a computer screen or prints the message into a hardcopy version. This classification applies to the file, not to Outlook or to the computer monitor or to the printer. If, however, information displayed is confidential, then precautions must be taken to protect its unauthorized view regardless of the method in which it is displayed. This document outlines the Iowa Lottery Authority's guidelines regarding the classification, protection, storage and disposal of data. These guidelines apply to employees' use of data at any Iowa Lottery Authority office, while in transit, and at alternate work sites.

AUTHORITY

This standard implements the requirements of the Iowa Lottery Authority Security Policy which states that a data classification hierarchy be established to delineate proper protection procedures.

AUDIENCE

This classification applies to all data maintained on Iowa Lottery Authority managed devices.

The impact of this standard could be significant. Implementation will require that every data file be examined in order to identify the level of security needed and thus a classification applied.

Iowa Lottery Authority
DATA CLASSIFICATION STANDARD

DATA CLASSIFICATION STANDARD

Please note that data and information are synonymous in the descriptions below and are used interchangeably to mean the same thing.

Classification is important because it determines the level of security to be applied to the data, the application that processes the data, and the environment which houses/stores the data. As would be expected, confidential data requires the most stringent security, sensitive requires less control than confidential but more control than public; while public data requires very little security (only controls over the integrity of the data are necessary). Classification can be determined by the following:

CONFIDENTIAL	SENSITIVE	PUBLIC
Any information that if lost, corrupted, or disclosed to or accessed by an unauthorized person may cause harm, injury, damage, or significant financial loss to another person or entity or which may corrupt the organization's mission.	Any information that if lost, corrupted, or disclosed to or accessed by an unauthorized person may cause embarrassment, humiliation, or dishonor to another person or entity.	Any information that if lost or disclosed to or accessed by any individual will, without question, <i>not</i> harm, damage, hurt, embarrass, humiliate, dishonor, or cause financial loss to another person or entity.
Any information or record deemed confidential under Section 22.7 of Chapter 22 of the Iowa Code, also known as the Iowa Open Records Law.	Any information that is requested as requiring completion of a formal request prior to release to the requesting individual.	Any information that is requested not requiring a formal request prior to publication accessible by the general public.
All <u>protected health information</u> as defined by <u>HIPAA</u>		
Information containing personal, private data on employees, contractors, or clients.		
Information that if disclosed or accessed by unauthorized means or persons or if lost or corrupted would violate state or federal law.		

Iowa Lottery Authority
DATA PROTECTION STANDARD

Security Measures

Appropriate technical and organizational measures must be put in place to prevent the unauthorized or unlawful processing or disclosure of data. Departments must ensure that the security measures in terms of physical security (e.g. control access to buildings or rooms, correct handling and disposal of printed material containing personal data), administrative controls (e.g. restrict password, restrict access on the basis of role or authority), and technical controls (e.g. store personal data on a secure server, make use of privacy enhancing technologies) are appropriate for the data being processed and maintained.

Security measures implemented for data will be dictated by the data classification level. Measures will include, but not be limited to, an appropriate combination of the following:

- Physical Access Control
- Administrative Access Control
- Technical Access Control

Handling Guidelines

Protected Confidential level information should not be stored within shadow systems (e.g. files, home-grown databases, spreadsheets, documents, and tables)

If there is a compelling reason to store this information within a shadow system, the system needs to be identified and appropriate controls need to be in place commensurate with the primary source of the confidential information.

Protected Confidential level information should not be sent, transmitted, or disseminated in an unsecured manner. The medium used to send, transmit or disseminate confidential information should be appropriately protected from modification or disclosure.

Procedures regarding the archival and destruction of, at a minimum, confidential and sensitive data should be implemented (e.g. Records Retention Policy)

It is recommended that data exchanges be executed through networks (electronically) rather than through physical media such as diskettes, CD's, tape, manual reports, etc. This eliminates the human error of delivering, and/or lost media that may put the lottery in a compromising position.

Definitions

- Alternate work sites include all work locations outside the Iowa Lottery
- In transit includes stops at all locations involved in reaching a final destination, such as traveling first to a retailer, then to the hotel, then to an Iowa Lottery office, etc.
- Portable storage devices (PSDs) include flash drives, CDs, DVDs, external hard drives, or any other form of electronic storage that can be removed from an Iowa Lottery office.
- Drives/Servers are referred to according to their type:
 - the C: drive
 - the D: drive
 - the server

General Data Handling Guidelines

- The guidelines detailed in the general and specific handling sections may not cover every possible situation. If a situation not covered in the guidelines is encountered, a supervisor must be contacted for further direction.
- Lottery employees will request and retain the minimum amount of confidential data required to carry out the Iowa Lottery Authority's mission. Any confidential data not necessary to conduct lottery operations must be redacted from all hardcopy and electronic records to limit exposure in case of loss.
- All hardcopy confidential data must be appropriately marked.
- The hierarchy below establishes the preferred approved methods, in priority order, of accessing confidential data outside an lottery office:
- Lottery policy requires that, **unless deemed necessary**, confidential data not leave an Iowa Lottery office or be accessed remotely.
- If using confidential data outside an Iowa Lottery office is deemed necessary, the approved method of accessing the confidential data are via direct logon to the Iowa Lottery domain through a VPN. However, employees must not print confidential data or download confidential data to local drives or PSDs without specific written permission.
- If VPN to direct logon to the lottery domain is not available, the next safest method of accessing confidential data is to remove it from the lottery office via a PSD or hard drive using appropriate lottery encryption methods, according to the State of Iowa Laptop Data Protection Standard and the State of Iowa Removable Storage Encryption Standard. Because confidential data is being removed from a lottery office, specific written approval is required.
- As a last resort, hardcopy confidential data may be transported outside a lottery office, with specific written approval. Hardcopy confidential data should remain in the direct possession of the employee or, if absolutely necessary, it must be secured in a locked container/room and stored out of public sight. Hardcopy confidential data can be mailed through an approved mail delivery service to an alternate work site.
- To remove confidential data from a lottery office, employees must obtain specific written approval for each instance from both a supervisor and a VP. (See section on Approval Process for Removing Confidential Data from an Iowa Lottery Office) Prior to approval, CEO/VPs must carefully weigh the need to remove confidential data from the office against the risk of loss. CEO/VPs should also give particular attention to requests to remove hardcopy confidential data since hardcopy cannot be encrypted to protect the data in case of loss.
- Confidential data may not be transmitted via e-mail unless it is encrypted through the use of Public Key Infrastructure, commonly referred to as PKI.

- Confidential data or Proprietary information may not be stored on hard drives or PSDs when not in transit or at an alternate work site.
- Confidential data or Proprietary information or laptops may not be checked as baggage.
- Only lottery furnished equipment may be used in conducting lottery activities involving confidential data or accessing lottery resources remotely via VPN direct log on to the lottery domain.
- When using lottery PCs in lottery offices, password-protected screensavers must be configured to activate after 5 minutes of inactivity. The screensaver must be activated manually when the workstation is unattended.
- When using lottery equipment (laptops) outside lottery offices, password-protected screensavers must be configured to activate after 5 minutes of inactivity. The screensaver must be activated manually when the workstation is unattended.
- Laptops must be locked to an immovable object when left in a location where an unauthorized person may gain access. This includes locking laptops when in a lottery office.
- Employee personal network drives may be used for interim working files, but the server network drive should be used for permanent storage of final documentation.
- Employees may retain interim hardcopy working files at their desks, but the designated secure record storage room should be used for permanent storage of final hardcopy documentation.
- When in an uncontrolled environment, employees must guard against disclosure of confidential and Proprietary data through eavesdropping/overhearing, social engineering, or overlooking by unauthorized persons.
- The only copy of an electronic file should not be removed from network drives and stored on hard drives or PSDs because they are not subject to normal data backup procedures and are at risk of loss. Rather, employees should “copy” an electronic file to hard drives and PSDs using standards appropriate to the type of data being copied. Upon return from an alternate work site, employees should transfer any data from hard drives or PSDs back to network drives.
- Employees are not authorized to destroy final documentation stored in the respective lottery secure records storage room or on the server network drive.
- Employees must immediately, within 1 hour, report any theft, loss, or compromise of confidential data or any device used to transport, access, or store lottery information to their supervisor.
- Employees may not share sensitive information with unauthorized persons.

Data Handling – Electronic Media						
Classification	Interim Documentation: Protection, Storage & Disposal				Final Documentation: Protection, Storage & Disposal	
	On-Site (Lottery Office)	Off-Site		Disposal	Storage On-Site	Disposal
		In Transit	Alternate work site			
Confidential	Data should be stored on restricted access folders on the network server. The server is AASTORE and the partition is the F drive.	Data may be transported on portable media or on the hard drive on laptops if encrypted in accordance with lottery encryption procedures. Electronic data should remain in the employee's direct possession. If absolutely necessary, it may be locked in a secure container, out of public site.	VPN access to data or direct log on to the lottery domain is the preferred method to access electronic confidential data. Any data accessed must be encrypted. Electronic data should remain in the employee's direct possession. If absolutely necessary, it may be locked in a secure container, or in a locked room, and stored out of public site.	Upon return from alternate work sites, transfer data from encrypted portable media and hard drives, to restricted access folders on the network server. CDs and floppy disks should be returned for destruction. Interim electronic data not required to be maintained in final documentation records storage (i.e. working copies of files) should be deleted from network server folders using "shift + Delete" keys.	Data should be maintained on restricted access folders on the network server. Any electronic data permanently stored on portable media should be encrypted, appropriately marked as confidential, and placed in the secure records storage room.	After appropriate record retention requirements are met, final documentation will be destroyed in a manner rendering it unreadable, undecipherable, and irretrievable.

Sensitive	Data should be stored on restricted access folders on the network server.	Data should be handled in a manner providing reasonable assurance that unauthorized persons do not gain access – such as securing portable media and laptops in a locked container.	Data should be handled in a manner providing reasonable assurance that unauthorized persons do not gain access – such as securing portable media and laptops in a locked container, or a locked room, or a locked residence when not in use.	Upon return from alternate work sites, transfer data from encrypted portable media and hard drives, to restricted access folders on the network server. CDs and floppy disks should be returned for destruction. Interim electronic data not required to be maintained in final documentation records storage (i.e. working copies of files) should be deleted from network server folders using “shift + Delete” keys.	Data should be maintained on restricted access folders on the network server. Any electronic data permanently stored on portable media should be appropriately placed in the secure records storage room.	After appropriate record retention requirements are met, final documentation will be destroyed in a manner rendering it unreadable, undecipherable, and irretrievable.
Public	No restrictions.	No restrictions.	No restrictions.	No restrictions.	No restrictions.	No restrictions.

Approval Process for Removing Confidential Data from a Iowa Lottery Office

Lottery employees transporting confidential data or using it at an alternate work site must obtain written supervisory approval using the attached request form. The employee should complete the form for specific authority to transport or use data at an alternate work site for each instance of removing confidential data from a lottery office.

Employees should send request to the appropriate supervisor. Supervisors should carefully consider the need to remove the confidential data prior to approving the request. If the team supervisor is not available, the request should be forwarded to the respective VP for approval. Lottery CEO can grant specific authority at any time.

Upon return to the lottery office, employees must sign the return certification statement signifying the return of the confidential data to the office and certifying the data was appropriately removed from hard drives and PSDs. Supervisors are ultimately responsible for ensuring employees sign the return certification form. Supervisors must maintain the completed form with all appropriate signatures for 1 year after the return certification is signed by the employee.

Confidential Data Removal Form

Date of Request				
Requested By				
Information Being Removed				
Description (list name of report(s) or file path of folder)	Laptop Hard Drive	Flash Drive	CD - DVD	Hard-Copy
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Purpose for Removal				
Dates and Location				
From	To	Location		

Certification statement

I have redacted electronic and hard copy confidential data as appropriate. I have encrypted electronic confidential data using approved methods. I have read and understand the guidelines in the Iowa Lottery Data Classification and Handling Procedures.

Name		Date	
-------------	--	-------------	--

Approval CEO/Vice President

Name		Date	
-------------	--	-------------	--

Return Certification Statement

I returned the confidential data listed on this request to the lottery office, appropriately removed confidential data from my laptop hard drive and portable media, and shredded paper copies no longer needed.

Name		Date	
-------------	--	-------------	--