STATE OF OKLAHOMA
CYBER COMMAND

Confidential Data

Data should be classified as *Confidential* when the unauthorized disclosure, alteration or destruction of that data could cause a severe or catastrophic level of risk to the State, agencies or our citizens. Examples of *Confidential* data include data protected by state or federal privacy regulations and data protected by confidentiality agreements. The highest level of security controls should be applied to *Confidential* data.

CONFIDENTIAL INFORMATION

- Will personal information be collected, contained or returned (PII)?
- Does the project involve sensitive information (example: formulas, employee information or financial data)?
- What is the highest level agency-sensitive information handled by the asset (Circle one)
  [Public] [Private] [Confidential] [Secret]
- Can a failure of this system lead to a physical injury or environmental impact?

Security Categorization and Risk Assignment

There must be a definition of impact and the degrees of potential impact to the state should there be a breach of security or disclosure of data. There are three security objectives to assess risk by:

Confidentiality

> *"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec 3542] A loss of confidentiality is the unauthorized disclosure of information.*

Integrity

> *"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542] A loss of integrity is the unauthorized modification or destruction of information.*

Availability

> *"Ensuring timely and reliable access to and use of information…" [44 U.S.C., Sec. 3542] A loss of availability is the disruption of access to or use of information.*

There are three levels to assign a risk metric to; they are defined as **Low**, **Moderate**, and **High**. The highest risk data must dictate the categorization.

Low impact: is the potential for the loss of confidentiality, integrity, or availability could be expected to have no or a limited adverse effect on agency operations, assets, or clients or employees.

> *A limited adverse effect means that, the loss of confidentiality, integrity or availability does not violate federal or state laws, meet the definition of a disclosure by law and have little to no degradation in agency mission capability, little to minor impact on agency assets; result in a minor financial loss; or result in little to no or minor harm to individuals.*

Moderate impact: is the potential for the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on agency operations, assets, or clients or employees.

> *A serious adverse effect means that, the loss of confidentiality, integrity or availability violates federal or state laws, meets the definition of a disclosure by law and cause a significant degradation in agency mission capability, significant impact on agency assets; result in a significant financial loss; or result in significant harm to individuals that does not involve loss of life or serious life threatening conditions.*

High impact: is the potential for the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on agency operations, assets, or clients or employees.

> *A severe or catastrophic adverse effect means that, the loss of confidentiality, integrity or availability violates federal or state laws, meets the definition of a disclosure by law and cause a severe degradation in agency mission capability, severe impact on agency assets; result in a severe financial loss; or result in severe harm to individuals that could involve loss of income, life, or serious life threatening conditions.*

Risk Assignment

The security categorization of information must follow the following process, of determining the information type and the impact on the confidentiality, integrity, and availability. Identification must be completed of the information type and assessment of the impact to confidentiality, integrity, and availability.

Security Categorization (Information Type) = for example "public information"

Confidentiality	Low	Moderate	High	N/A
Integrity	Low	Moderate	High	N/A
Availability	Low	Moderate	High	N/A

The resulting review would assign an impact based on review of the information type; the review would be expressed as:

SC (Public information) = {(Confidentiality, N/A), (Integrity, Low), (Availability, Low)} the resulting risk value for public information would be Low.

SC (Personally Identifiable Information) = (Confidentiality, Moderate), (Integrity, Moderate), (Availability, Moderate)} the resulting risk value for public information would be Moderate.

Identification of Risk Assignment

Complete this section* to provide the security classification of agency data by entering the Information type and identifying the impact to Confidentiality, Integrity, and Availability from the criteria set forth in the above, the first line is an example only. If you have regulated data, you can find the Risk Assignment in the regulatory environment section below, it has been completed for you. This is also the section where you must document the required retention, in years that the data must be kept. The Oklahoma Records Management Act outlines the requirements for adapting a records retention schedule.

Information Type \ Location	Impact to Confidentiality	Impact to Integrity	Impact to Availability	Security Classification	Retention (in years)	Data Classification	Data Storage Options
Public Information *\\server1\groupA\folder1*	*N/A*	*Low*	*Low*	***Low***	***7***	***Public***	***Public Hosted***

*The Data Classification and Security Categorization Excel Workbook should be used for more detailed information gathering and reporting. The chart above is for explanatory purposes.

REGULATORY ENVIRONMENTS

- Do systems store, process or display customer credit cards (PCI)?
  - Security Classification = Moderate
- Do systems store, process or display financial information (GLBA)?
  - Security Classification = Moderate
- Do systems store, process or display healthcare information (HIPAA)?
  - Security Classification = Moderate
- Do systems store, process or display student education information (FERPA)?
  - Security Classification = Moderate
- Do systems store, process or display federal taxpayer information (IRS-1075)?
  - Security Classification = High
- Do systems store, process or display criminal history record information (CHRI) (CJIS)
  - Security Classification = High
- Do systems store, process or display Social Security Administration (SSA) data files received from the SSA?

    - Security Classification = Moderate
- Do systems store, process, or display Credit Card data (PCI-DSS)?
    - Security Classification = Moderate
- Do systems store, process, or display banking or financial data related to bank accounts (PCI-DSS)?
    - Security Classification = Moderate

Security Categorization Mapping to Regulated Data

This section is the identified risk assignment, security categorization and data classification for the listed regulated data sets. The risk assignment provides the security classification of data by entering the Information type and identifying the impact to Confidentiality, Integrity, and Availability. The provided chart below has been completed for the state based on these regulations by using information provided by the National Institute of Standards and Technology (NIST) and the published risk assignment by the Federal Government Accountability Office (GAO).

Information Type	Impact to Confidentiality	Impact to Integrity	Impact to Availability	Security Classification	Data Classification
Credit Card Data & Banking Data (PCI-DSS)	*Moderate*	*Moderate*	*Moderate*	***Moderate***	***Confidential - Regulatory***
Electronic Health Information (ePHI / HIPAA)	*Moderate*	*Moderate*	*Moderate*	***Moderate***	***Confidential - Regulatory***
Student Record Data (FEPRA)	*Moderate*	*Moderate*	*Moderate*	***Moderate***	***Confidential - Regulatory***
Federal Taxpayer Information (FTI / IRS-1075)	*Moderate*	*Moderate*	*Moderate*	***Moderate***	***Specialized - Regulatory***
Social Security Administration Data (SSA)	*Moderate*	*Moderate*	*Moderate*	***Moderate***	***Confidential - Regulatory***
Criminal History Record Information (CHRI - CJIS)	*High*	*High*	*Moderate*	***High***	***Specialized - Regulatory***

Data Storage Options

The Data Storage Options identify where the data can be stored. This will help identify solutions and requirements for meeting the growing demands for data storage needs for the state. The options are:

State Datacenter Storage (On Prem): This identifies that the data must only be stored within the state data center and should not be considered for any hosted storage. This should apply to highly transaction intensive data storage and usage, highly sensitive data, or data that by any agreement, regulation, or state statute should not be stored in a hosted solution.

Public Hosted: This identifies that the data does not have any regulatory requirements, does not contain any personally identifiable information, and no state sensitive data that could be used to compromise a state system, such as technical information, user names, and employee data. This information is classified as Public data.

Confidential / Regulatory Hosted: This identifies that the data does have sensitive data elements and is regulated. This data must be stored in a FedRAMP certified hosted solution and should have all the controls in place to meet the regulatory requirements.

CJIS and FTI Specialized Regulatory Hosted: This identifies that the data does have Criminal History Record Information or Federal Taxpayer Information that is received from the IRS. This data must be stored in a FedRAMP and CJIS, and IRS 10-75 approved hosted solution.

Private Data

Data should be classified as *Private* when the unauthorized disclosure, alteration or destruction of that data could result in a significant level of risk to the State, agencies or our citizens. By default, all Institutional Data that is not explicitly classified as *Confidential* or *Public* data should be treated as *Private* data. A moderate level of security controls should be applied to *Private* data.

Private data can include:

- Information Technology (IT) drawings, diagrams, models, make, operating systems, versions, security and risk assessments, account user names and Internet Protocol (IP)addresses.
- Intellectual Property (IP) software code, trademarks, copyrights, patents, industrial designs, or otherwise intangible asset data that would if disclosed result in a significant level of risk .
- Facilities information such as building layout and design, HVAC systems, environmental monitoring systems, security systems, physical locations of technology, file storage, sensitive processing of information, and emergency evacuation routes.

Public Data

Data should be classified as *Public* when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the State, agencies or our citizens. Examples of *Public* data include press releases, and CIO annual reports. While little or no controls are required to protect the confidentiality of *Public* data, some level of control is required to prevent unauthorized modification or destruction of *Public* data.

Agency-Specific Data Classification Handling

The following pages contain recommended guidelines to assist your agency in handling data that has been classified. Your agency should modify this information to fit your security needs, audit requirements, and risk appetite. In addition to these guidelines, any data covered by federal or state laws or regulations or contractual agreements must meet the security requirements defined by those laws, regulations and/or contracts.

	Information Classifications			
	Public (LOW)	**Private (Moderate)**	**Confidential / Regulatory (Moderate)**	**Specialized Regulatory (High)**
Access Controls	No restriction for viewing Authorization of data owner or designee required for modification	Viewing and modification restricted to authorized individuals as needed for business-related role Data Owner or designee grants permission for access, plus approval from supervisor Authentication and authorization required for access	Viewing and modification restricted to authorized individuals as needed for business-related role Data Owner or designee grants permission for access, plus approval from supervisor Authentication and authorization required for access Confidentiality agreement required	Same as Moderate
Copying/Printing	No restrictions	Data should only be printed when there is a legitimate need Copies must be limited to individuals with a need to know Data should not be left unattended on a printer/fax May be sent via inter-agency mail	Data should only be printed when there is a legitimate need Print with a PIN to prevent unauthorized viewing Copies must be limited to individuals authorized to access the data and have signed a confidentiality agreement Data should not be left unattended on a printer/fax Data must be marked "Confidential" Must be sent via Confidential envelope Hardcopies must be stored in a secure location	Same as Moderate

	Information Classifications			
	Public (LOW)	**Private (Moderate)**	**Confidential / Regulatory (Moderate)**	**Specialized Regulatory (High)**
Network Security	May reside on a public network Firewall protection recommended IDS/IPS protection recommended Protection only with router ACLs acceptable	Firewall protection Required IDS/IPS protection recommended, host-based recommended Protection with router ACLs optional Servers hosting the data should not be visible to the entire internet May be in a shared network server subnet with a common firewall ruleset for the set of servers	Protection with a network using "default deny" ruleset required Host-based IDS/IPS protection required Protection with router ACLs optional Servers hosting the data must not be visible to the entire internet, not to unprotected subnets like Oklahoma Open Must have a firewall ruleset dedicated to the system The firewall ruleset must be reviewed periodically	Same as Moderate
System Security	Must follow best practices for system management and security Host-based software firewall required	Must follow state policy and OS-specific best practices for system management and security Host-based software firewall required Host-based IDS/IPS recommended Servers must be patched to current level Annual risk review required Quarterly vulnerability scan recommended	Must follow state policy and OS-specific best practices for system management and security Host-based software firewall required Host-based IDS/IPS required Servers must be patched to current level Annual risk review required Quarterly vulnerability scan required	Same as Moderate

	Information Classifications			
	Public (LOW)	**Private (Moderate)**	**Confidential / Regulatory (Moderate)**	**Specialized Regulatory (High)**
Virtual Environment	May be hosted in a virtual environment All other security controls apply to both the host and guest VMs	May be hosted in a virtual environment All other security controls apply to both the host and guest VMs Should not share the same virtual host environment with guest virtual servers of other security classifications	May be hosted in a virtual environment All other security controls apply to both the host and guest VMs Cannot share the same virtual host environment with guest virtual servers of other security classifications	Same as Moderate
Physical Security	System must be locked or logged out when unattended Host-based firewall recommended	System must be locked or logged out when unattended Hosted in a secure location required; a Secure Data Center is recommended	System must be locked or logged out when unattended Hosted in a Secure Data Center is required Physical access must be monitored, logged and limited to authorized individuals 24x7	Same as Moderate
Remote access to systems hosting the data	No restrictions	Access restricted to local area network or VPN Remote access by third party for technical support limited to authenticated, temporary access via direct dial-in modem or secure protocols over the internet	Restricted to local network or secure VPN group Unsupervised remote access by third party for technical support not allowed Two-factor authentication recommended	Same as Moderate
Data Storage	Storage on a secure server recommended Storage in a secure data center recommended	Hosted in a secure location is required; Storage in a secure data	Hosted in Secured Data Center Required Physical access must be monitored, logged and limited	Same as Moderate

	Information Classifications			
	Public (LOW)	**Private (Moderate)**	**Confidential / Regulatory (Moderate)**	**Specialized Regulatory (High)**
		center recommended Do not store on an individual's workstation or mobile device	to authorized individuals 24x7 Must not be stored on an individual's workstation or mobile device	
Transmission	No restrictions	Restricted to Exchange environment using Information Rights Management to authenticate sender and recipient and prevent forwarding.	Encryption required (for example via SSL or secure file transfer protocols) Cannot transmit via email unless encrypted and secured with a digital signature	Same as Moderate
Backup/Disaster Recovery	Daily backups recommended Off-site storage recommended	Daily backups required Off-site storage recommended	Daily backups required Off-site storage in a secure location required Encryption on backup media recommended	Same as Moderate
Media Sanitation and Disposal	No restrictions	Shred reports Wipe/erase media Follow state policy for Secure Erase procedure	Secure shred reports Destroy electronic media Follow state policy for Data Destruction procedure	Same as Moderate
Auditing	Not needed	Logins	Logins, access and changes	Same as Moderate
Laptops	May reside on non-state IT assets. (All state assets must, by state law, have laptop encryptions, and strong passwords)	Strong passwords, Lock laptops when not in use Hard Drive encryption	Strong passwords, Lock laptops when not in use Hard Drive encryption Do not use in public places (e.g. airports and airplanes)	Same as Moderate
Mobile Devices	No special requirements, BYOD permitted	Do not use except on approved,	Do not use	Same as Moderate

	Public (LOW)	Private (Moderate)	Confidential / Regulatory (Moderate)	Specialized Regulatory (High)
		OMES-managed devices, OMES managed infrastructure		
Telephone	No special requirements	No special requirements	Must have certification to comply with applicable regulatory requirements	Same as Moderate
Voicemail	No special requirements	Only recorded on voicemail systems that conform to state policy	Do not use unless a regulatory-approved technology (e.g. a PCI-certified IVR system) is employed.	Same as Moderate
Training	General security awareness training required	General security awareness training required Data Security training required	General security awareness training required Data Security training required Applicable policy and regulatory training required	Same as Moderate
Cloud	No special requirements	Can only be posted on Intranet sites or externally with appropriate access controls	Must use the Confidential and Regulatory Cloud	Must use the CJIS and FTI Cloud

ACCEPTANCE FORM

Data Classification, Security Categorization, Data Retention, and Storage

I have carefully assessed the Data Classification, Security Categorization, Data Retention and Storage requirements. I fully accept the documented classification and categorizations and authorize the Office of Management and Enterprise Services to utilize this information in the performance of their duties.

_____ _____

(State Agency Director or Designee) DATE