admin
THE SOUTH CAROLINA
DEPARTMENT of ADMINISTRATION

South Carolina Division of State Human Resources

InfoSec & Privacy Workforce

Data Classification Roles and Responsibilities

Start

Introduction

The Data Classification Roles and Responsibilities Toolkit for the State of South Carolina (State) is designed to help agencies adopt Information Security (InfoSec) and Privacy roles and responsibilities statements.

Consistent and clearly defined roles and responsibilities will create accountability and ownership of InfoSec and Privacy roles at each State agency, and in turn improve InfoSec and privacy compliance and competency.

Within the toolkit, you will find:

- An **overview of the InfoSec and Privacy roles** that includes definitions and their associated responsibilities. This will enable State personnel (technical and non-technical) who perform these roles to understand expectations, uphold compliance, and increase ownership of increasing the State's security posture
- A **tier categorization** that can be used as a guide to determine the minimum number of Full-Time Equivalents (FTEs) needed to complete the tasks with the associated roles
- **Guidelines to applying roles within agencies** that highlight specific areas to consider when adopting these roles
- A set of **role scenarios** using select agencies as examples. These examples illustrate how they are intended to support agency adoption and implementation of newly defined roles and responsibilities

Continue to InfoSec and Privacy Roles

InfoSec and Privacy Roles

Eleven InfoSec and Privacy roles were developed by taking into consideration the State's current approach to InfoSec and privacy and the State's data classification schema[1]. *Click each role to see the associated roles and responsibilities statements.*

[1] Click here to see an overview of the State's data classification schema

	InfoSec and Privacy Roles
Oversight & Governance	Policy Champion
	Compliance Liaison
	Privacy Liaison
	Security Liaison
	Data Owner
	System Owner
Security Operations	Incident Manager / Responder
	Data Custodian
	System Administrator
User Groups	System User
	Data User

Continue to Tier Categorization

Tier Categorization

Agencies will be responsible to fill all roles, however, multiple roles can be fulfilled by the same Full-Time Equivalent (FTE). These roles will not necessarily require a significant portion of the FTE's time. The proposed tiers below are a guide to determine the minimum number of FTEs needed to fill these roles.

Agency Considerations
Choose the highest tier based on the following two criteria: **1. Data Sensitivity**[1] • Restricted → Tier 3 • Confidential → Tier 2 • Internal Use/Public → Tier 1 **2. User Size**[2] • > 2501 → Tier 3 • 901 - 2500 → Tier 2 • 0 - 900 → Tier 1

Tier	Criteria	Minimum # FTEs
Tier 3	**Data Sensitivity**: Restricted and/or **Users**: > 2501	2 FTEs
Tier 2	**Data Sensitivity**: Confidential and/or **Users**: 901 – 2500	1 FTE
Tier 1	**Data Sensitivity**: Internal Use/Public and/or **Users**: 1 – 900	0.25 FTE

[1] Data custodians and users of Personal Health Information (PHI) must adhere to additional responsibilities including those commensurate with HIPAA regulations

[2] Increased number of users within a tier may require Agency to utilize more than the minimum recommended number of FTEs

Back to InfoSec and Privacy Roles

Continue to Guidelines

Guidelines

The following guidelines should be taken into consideration when applying the InfoSec and Privacy roles within State agencies.

- **Role Allocation** is determined by the agency's existing workforce, InfoSec and Privacy needs, and tier identification
  - Roles can be shared by employees within an agency or with support from other agencies, the Division of Information Security (DIS), or the Enterprise Privacy Office (EPO) as needed
  - Using support from other agencies depends on shared systems, agency locations, data sensitivity, and other factors
  - While roles can be shared across agencies, it is critical to ensure the minimum number of FTEs are filled based on the agency's tier
- **Segregation of Duties** is recommended to instill checks and balances where possible and eliminate conflicts of interest
  - The primary segregation of duties shall occur between roles under ***Oversight & Governance*** and ***Security Operations***
  - It is recommended that the roles of Policy Champion, Compliance Liaison, Incident Manager/Responder, and Privacy Liaison be executed by an individual distinct from the employee owning the data or system
    - *For example:* If an employee is a data owner, they should not be responsible for compliance checks. This avoids a potential conflict of interest
- **Data and System Users** include any stakeholder (State employee, contractor, or vendor) who has access to State data. Data and System Users have a shared responsibility to InfoSec and privacy through compliance with established InfoSec and Privacy policies

Back to Tier Categorization

Continue to Role Scenario Roadmap

Role Scenario Roadmap

Five sample Role Scenarios have been developed to illustrate the adoption of Roles and Responsibilities based on agency characteristics. These examples are not inclusive of all potential scenarios but serve as guidance for adoption. *Click on the sample Role Scenarios below to explore these examples.*

Role Scenario Example	Agency Description	
	Data Sensitivity	User Base
Role Scenario 1	Restricted	5,000
Role Scenario 2	Confidential	75
Role Scenario 3	Internal/Public Use	600
Role Scenario 4	Restricted	200
Role Scenario 5	Internal/Public Use	3,000

Please refer to the Tier Categorizations for further details when determining the appropriate tier or contact your HR Consultant with any questions

Back to Guidelines

Continue to Mapping of Roles to Positions

Roles Scenario 1

The example below shows how an Agency can tailor these roles to their resources.[1]

Agency A

Agency A Profile[2]

Data Sensitivity: Restricted
User Base: 5,000

Tier

Agency A has "restricted" data and more than 2501 employees; therefore, it falls under **Tier 3**

Minimum # FTEs

2 FTEs. Examples of FTEs allocation:

Example A:
- 1 FTE, 1 Person
- 1 FTE, 1 Person

Example B:
- 0.5 FTE, 1 Person
- 0.5 FTE, 1 Person
- 1 FTE, 1 Person

Roles Allocation

Inter-Agency Roles

- Policy Champion
- Compliance Liaison
- Data Owner
- Data Custodian
- System Owner
- System Administrator
- Incident Manager / Responder
- Security Liaison
- Privacy Liaison

Intra-Agency Roles

- N/A

In this example, this Agency has filled the InfoSec and Privacy roles internally.

Alternatively, the Agency can request support from agencies, DIS, or EPO to fill the roles. This decision is based on existing workforce availability and InfoSec and Privacy needs, along with other factors.

[1] For illustrative purposes only

[2] Agencies may allocate roles differently based on existing Agency workforce, InfoSec and Privacy needs, tier identification, data systems, and network setup

Back to Tier Categorization
Back to Role Scenario Roadmap
Continue to Mapping of Roles to Positions

Roles Scenario 2

The example below shows how an Agency can tailor these roles to their resources.[1]

Agency B

Agency B Profile[2]

Data Sensitivity: Confidential
User Base: 75

Tier

Agency B has "confidential" data; therefore, it falls under **Tier 2**

Minimum # FTEs

1 FTE. Examples of FTE allocation:

Example A:
- .5 FTE, 1 Person
- .5 FTE, 1 Person

Example B:
- .75 FTE, 1 Person
- .25 FTE, 1 Person

Roles Allocation

Inter-Agency Roles

- Policy Champion
- Compliance Liaison
- Data Owner
- Incident Manager / Responder
- Security Liaison
- Privacy Liaison

Intra-Agency Roles

- Data Custodian
- System Owner
- System Administrator

In this example, the Agency has shared InfoSec roles with other agencies, DIS, or EPO.

[1] For illustrative purposes only

[2] Agencies may allocate roles differently based on existing Agency workforce, InfoSec and Privacy needs, tier identification, data systems, and network setup

Back to Tier Categorization
Back to Role Scenario Roadmap
Continue to Mapping of Roles to Positions

Roles Scenario 3

The example below shows how an Agency can tailor these roles to their resources.[1]

Agency C

Agency C Profile[2]

Data Sensitivity: Internal Use / Public

User Base: 600

Tier

Agency C has "internal use and public" data and less than 900 users; therefore, it falls under **Tier 1**

Minimum # FTEs

.25 FTE. Examples of FTE allocation:

Example A:

- .25 FTE, 1 Person

Roles Allocation

Inter-Agency Roles

- Policy Champion
- Compliance Liaison
- Data Owner
- Incident Manager / Responder
- Security Liaison
- Privacy Liaison
- Data Custodian

Intra-Agency Roles

- System Owner
- System Administrator

In this example, the Agency has shared InfoSec roles with other agencies, DIS, or EPO.

[1] For illustrative purposes only

[2] Agencies may allocate roles differently based on existing Agency workforce, InfoSec and Privacy needs, tier identification, data systems, and network setup

Back to Tier Categorization

Back to Role Scenario Roadmap

Continue to Mapping of Roles to Positions

Roles Scenario 4

The example below shows how an Agency can tailor these roles to their resources.[1]

Agency D

Agency D Profile[2]

Data Sensitivity: Restricted
User Base: 200

Tier

Although Agency D only has a user base of 200, it has "restricted" data and therefore falls under **Tier 3**

Minimum # FTEs

2 FTEs. Examples of FTEs allocation:

Example A:
- 1 FTE, 1 Person
- 1 FTE, 1 Person

Example B:
- 0.5 FTE, 1 Person
- 0.5 FTE, 1 Person
- 1 FTE, 1 Person

Roles Allocation

Inter-Agency Roles

- Policy Champion
- Compliance Liaison
- Data Owner
- Incident Manager / Responder
- Security Liaison
- Privacy Liaison

Intra-Agency Roles

- Data Custodian
- System Owner
- System Administrator

In this example, the Agency has shared InfoSec roles with other agencies, DIS, or EPO.

[1] For illustrative purposes only

[2] Agencies may allocate roles differently based on existing Agency workforce, InfoSec and Privacy needs, tier identification, data systems, and network setup

Back to Tier Categorization
Back to Role Scenario Roadmap
Continue to Mapping of Roles to Positions

Roles Scenario 5

The example below shows how an Agency can tailor these roles to their resources.[1]

Agency E

Agency E Profile[2]

Data Sensitivity: Internal Use / Public

User Base: 3000

Tier

Agency E has "internal use and public" data but has more than 2501 users; therefore, it falls under **Tier 3**

Minimum # FTEs

2 FTEs. Examples of FTEs allocation:

Example A:
- 1 FTE, 1 Person
- 1 FTE, 1 Person

Example B:
- 0.5 FTE, 1 Person
- 0.5 FTE, 1 Person
- 0.5 FTE, 1 Person
- 0.5 FTE, 1 Person

Roles Allocation

Inter-Agency Roles

- Policy Champion
- Compliance Liaison
- Data Owner
- Incident Manager / Responder
- Security Liaison
- Privacy Liaison

Intra-Agency Roles

- Data Custodian
- System Owner
- System Administrator

In this example, the Agency has shared InfoSec roles with other agencies, DIS, or EPO.

[1] For illustrative purposes only

[2] Agencies may allocate roles differently based on existing Agency workforce, InfoSec and Privacy needs, tier identification, data systems, and network setup

Back to Tier Categorization

Back to Role Scenario Roadmap

Continue to Mapping of Roles to Positions

Mapping of Roles to Positions

The table below provides insight into how each of the eleven roles may potentially map to select position descriptions (including technical and non-technical jobs) within the State.[1]

Roles \ Positions		InfoSec and Privacy Positions					IT Positions		Other Positions	
		InfoSec Analyst	InfoSec Manager	InfoSec and Privacy Auditor	Information Privacy Analyst	Information Privacy Manager	IT Director	Network Administrator	Agency Director	HR Manager
Oversight & Governance	Policy Champion		X			X	X			X
	Compliance Liaison	X	X	X			X	X		
	Security Liaison	X	X				X			X
	Privacy Liaison			X	X	X	X			
Security Operations	Data Owner				X	X			X	X
	Data Custodian	X	X				X	X		X
	System Owner						X			
	System Administrator						X			X
	Incident Manager / Responder	X	X		X	X	X	X		X
User Groups	System User	X	X	X	X	X	X	X	X	
	Data User	X	X	X	X	X	X	X		X

[1] For illustrative purposes only

Back to Tier Categorization
Continue to Summary

Summary

This presentation should be used as a guide when implementing the Roles and Responsibilities at each agency based on the data sensitivity and user base. The following are key takeaways:

- The detailed **InfoSec and Privacy Roles** were developed by taking into consideration the State's current approach to State's data classification schema
- A comprehensive **State of South Carolina Data Classification Schema** illustrates how data sensitivity is defined
- The **Tier Categorization Guide** helps determine the minimum number of FTEs needed to fill these roles based on agency's data sensitivity and user base
- Five different **Role Scenarios** illustrate the adoption of Roles and Responsibilities based on agency characteristics. These examples are not inclusive of all potential scenarios but serve as guidance for adoption.
- An illustrative **Mapping of Roles to Positions** depicts an example of how InfoSec and Privacy roles may map to select State position descriptions
- InfoSec and Privacy Position Descriptions have been created based on the roles and responsibilities identified in this presentation. These position descriptions can aid in the hiring of personnel, where appropriate, and have been distributed as a part of the InfoSec and Privacy Professional Development Program (PDP)

Please contact your PDP Manager or HR Consultant with any further questions

Appendices

Role Definition and Responsibility Statements

The following includes initial Position Description language associated with the Policy Champion role that could be incorporated into existing job documentation to ensure consistency while supporting compliance across the State.

Policy Champion

Role Definition

- Policy Champions serve as a liaison between Agency senior leadership team and DIS. They may hold a management role in the areas of compliance, privacy, InfoSec, and/or technology. This role reports up through the Agency to the Agency Director

Role Responsibilities

- Review, interpret and disseminate existing or new InfoSec and Privacy policies, standards, and guidelines for State data and/or systems within purview; develop additional Agency policies, as needed
- Lead policy implementation and management efforts within the Agency, including policy updates and compliance, and coordination with DIS
- Conduct gap analysis and document a policy implementation plan and roadmap
- Identify and resolve policy deployment challenges and risks

Position Description

- Contribute to the development, review, update and/or monitoring of InfoSec and Privacy policies, standards, and guidelines, in consultation with Agency leadership

Back to Overview of InfoSec and Privacy Roles

Role Definition and Responsibility Statements

The following includes initial Position Description language associated with the Compliance Liaison role that could be incorporated into existing job documentation to ensure consistency while supporting compliance across the State.

Compliance Liaison

Role Definition

- Compliance Liaisons implement and monitor InfoSec and Privacy policies, procedures and practices designed to ensure compliance with State requirements. Champions compliance activities and is responsible for audit, assessment, validation, and system monitoring to ensure compliance. This role reports up through the Agency to the Agency Director

Role Responsibilities

- Serve as a liaison between agencies and leadership to align compliance objectives with State obligations and requirements
- Assess security controls to determine the extent to which internal and external controls are implemented correctly, operating as intended, and producing desired compliance outcomes
- Develop and document auditing and monitoring plans, and provide an escalation path within the Agency for compliance related issues
- Raise and maintain compliance awareness within the Agency; communicate information on compliance priorities within the Agency, including conduct of compliance trainings
- Cascade State compliance-related messages to Agency senior leadership or personnel

Position Description

- Monitor Agency compliance with InfoSec policies and procedures, and facilitate resolution of or escalate issues to the appropriate leadership or personnel, as necessary

Back to Overview of InfoSec and Privacy Roles

Role Definition and Responsibility Statements

The following includes initial Position Description language associated with the Data Owner role that could be incorporated into existing job documentation to ensure consistency while supporting compliance across the State.

Data Owner

Role Definition

- Data Owners provide direct authority and control over the management and use of specific data that is transmitted, used, and stored on a system or systems within a department, function, or administrative unit of the State. This role reports up through the Agency to the Agency Director

Role Responsibilities

- Review and approve guidelines related to administrative and operational use of data
- Determine appropriate criteria for obtaining and sharing access to data based on function, role, etc.
- Assign appropriate classification (e.g., Public, Internal Use, Confidential, Restricted) to data assets based on its sensitivity, value and criticality to the State
- Anticipate, identify, and address risk related to threats (e.g., phishing) that impact the confidentiality, integrity and availability of data
- Provide oversight to Data Custodians responsible for the protection of the confidentiality, integrity and availability of data, ensuring compliance with approved policies and regulatory requirements as they relate to the information asset

Position Description

- Define policies and guidelines for proper use and release of data and information, including protection requirements for data based on sensitivity of the data, legal or regulatory requirements and Agency needs

Back to Overview of InfoSec and Privacy Roles

Role Definition and Responsibility Statements

The following includes initial Position Description language associated with the Data Custodian role that could be incorporated into existing job documentation to ensure consistency while supporting compliance across the State.

Data Custodian

Role Definition

- Data Custodians have administrative and/or operational responsibility over information assets and ensure the protection of sensitive data and intellectual property residing on systems for which they have accountability. This role reports up through the Agency to the Agency Director

Role Responsibilities

- Communicate guidelines to Data Users pertaining to the use, exchange, or display of content using internal or external communication channels (e.g., Google, Facebook, etc.) as permitted by the Agency
- Protect data in custody from unauthorized access, alteration, destruction or usage
- Understand and report how data is created, stored, processed and transmitted within and outside of the Agency (e.g., electronic or social media, recorded on paper)
- Provision and deprovision access to data, as authorized by Data Owner
- Understand how to recognize and report on security risks (e.g., illegal download of data)

Position Description

- Oversee the safe custody, creation, transmission, storage and use of data using physical and system security and safeguards appropriate to the classification level of the data in custody (e.g., firewalls, data encryption)

Back to Overview of InfoSec and Privacy Roles

Role Definition and Responsibility Statements

The following includes initial Position Description language associated with the Data User role that could be incorporated into existing job documentation to ensure consistency while supporting compliance across the State.

Data User

Role Definition

- Data Users have a critical role in the effort to protect and maintain State information systems and data. For purpose of InfoSec or privacy, a Data User is any employee, contractor or third-party provider authorized to access the State's information systems and/or information assets. This role reports up through the Agency to the Agency Director

Role Responsibilities

- Access and use data to fulfill authorized job duties or activities for the State, in adherence to policies and guidelines pertaining to data protection
- Practice responsible use of electronic communication channels such as social media in accordance to approved local policies and guidelines
- Report actual or suspected vulnerabilities in the confidentiality, integrity or availability of data to the appropriate authorities (e.g., aggregated social media posts, phishing)
- Report actual or suspected breaches in the confidentiality, integrity or availability of data to the appropriate authorities

Position Description

- Implement safeguards and adhere to policies and guidelines established by the Agency and appropriate Data Owners pertaining to the use of data only as required for the purpose of fulfilling assigned roles or functions within the Agency

Back to Overview of InfoSec and Privacy Roles

Role Definition and Responsibility Statements

The following includes initial Position Description language associated with the Systems Owner role that could be incorporated into existing job documentation to ensure consistency while supporting compliance across the State.

System Owner

Role Definition

- System Owners provide direct authority over development and management of systems operations and information access within a department, function, or administrative unit. This role reports up through the Agency to the Agency Director

Role Responsibilities

- Manage confidentiality, integrity and availability of systems for which they own
- Understand systems of record containing State or local information and secure information within systems based on classification to data assets assigned by Data Owners
- Develop, implement, and manage criteria for obtaining access to information systems, and other processes or controls in compliance with approved policies
- Advise leadership on the resources (e.g., financial, human) necessary to develop and implement information systems and controls, including those specifically required by grants or contracts
- Define information system risks and develop and/or maintain standards to address risks due to physical security threats and vulnerabilities (e.g., theft of equipment, accidental damage from electrical surges)

Position Description

- Coordinate the procurement, development, integration, modification, or operation and maintenance of an information system with appropriate units within an agency according to the agreed upon security requirements

Back to Overview of InfoSec and Privacy Roles

Role Definition and Responsibility Statements

The following includes initial Position Description language associated with the System Administrator role that could be incorporated into existing job documentation to ensure consistency while supporting compliance across the State.

System Administrator

Role Definition

- System Administrators oversee the levels of access designated to users from an administrative and operational perspective. They ensure that access controls provide the appropriate protection of systems (e.g., passwords, certifications for data types). This role reports up through the Agency to the Agency Director

Role Responsibilities

- Manage confidentiality, integrity and availability of systems for which they own
- Understand systems of record containing State or local information and secure information within systems based on classification to data assets assigned by Data Owners
- Develop, implement, and manage criteria for obtaining access to information systems, and other processes or controls in compliance with approved policies
- Advise leadership on the resources (e.g., financial, human) necessary to develop and implement information systems and controls, including those specifically required by grants or contracts
- Define information system risks and develop and/or maintain standards to address risks due to physical security threats and vulnerabilities (e.g., theft of equipment, accidental damage from electrical surges)

Position Description

- Manage day-to-day administration of systems, and implement security controls and other InfoSec and Privacy requirements on systems

Back to Overview of InfoSec and Privacy Roles

Role Definition and Responsibility Statements

The following includes initial Position Description language associated with the System User role that could be incorporated into existing job documentation to ensure consistency while supporting compliance across the State.

System User

Role Definition

- System Users have a critical role in the effort to protect and maintain local information systems and supporting infrastructure. A System User is any employee, contractor, or third party provider authorized to access the State's information systems and/or assets. They should be in compliance and informed of how to detect and respond to possible system violations. This role reports up through the Agency to the Agency Director

Role Responsibilities

- Comply with controls established by the System Owner and adopt appropriate measures to protect the integrity of systems and supporting infrastructure (e.g., do not share devices used for identification and authorization purposes)
- Practice responsible use of computer systems and information networks (e.g., standalone, intranet, local area networks) in accordance to approved policies and guidelines
- Report system incidents, including unintentional or intentional misuse
- Report actual or suspected breaches to protect systems and related supporting infrastructure against threats and hazards associated with their physical environment (e.g., unauthorized entry into buildings, unattended computing access)

Position Description

- Adopt reasonable and prudent steps to protect the security of IT systems and data to which individual uses only as required for the purpose of fulfilling assigned roles or functions within the Agency

Back to Overview of InfoSec and Privacy Roles

Role Definition and Responsibility Statements

The following includes initial Position Description language associated with the Incident Manager/ Responder role that could be incorporated into existing job documentation to ensure consistency while supporting compliance across the State.

Incident Manager / Responder

Role Definition

- Incident Managers / Responders have authority and control to manage prevention and reaction to InfoSec threats, vulnerabilities, and incidents across the state. Their timely, strategic response affects security and privacy of all systems and data. This role reports up through the Agency to the Agency Director

Role Responsibilities

- Monitor data and system compliance, determine and respond to any apparent outliers
- Respond to crisis or urgent situations to mitigate immediate and potential threats
- Use mitigation, preparedness, response and recovery approaches to maximize survival of life, preservation of property, and integrity of information systems and data
- Investigate and analyze all relevant response activities within the Agency to support prompt restoration and limit privacy impact in the event of a threat
- Coordinate incident documentation (e.g., lessons learned) and documentation retention activities

Position Description

- Lead and/or participate in the investigation and documentation of InfoSec breaches and policy violations and track to conclusion based on formal Agency procedure for internally reporting and tracking security incidents

Back to Overview of InfoSec and Privacy Roles

Role Definition and Responsibility Statements

The following includes initial Position Description language associated with the Security Liaison role that could be incorporated into existing job documentation to ensure consistency while supporting compliance across the State.

Security Liaison

Role Definition

- Security Liaisons serve as a point of contact for Agency leadership and State committees (e.g., governance committee), by applying their knowledge of relevant InfoSec policies and guidelines. They may hold a management role in technical areas (e.g., cyber security). This role reports up through the Agency to the Agency Director

Role Responsibilities

- Serve as the primary point of contact at the Agency for security related requests, issues, and communication
- Coordinate with the State and Agency senior leadership to establish policies, procedures, and education regarding InfoSec within the Agency
- Facilitate requests for access to information systems (e.g., obtain proper approval, determine appropriate access needs for personnel)
- Monitor all authorized access to systems and supporting infrastructure to agency personnel; detect and investigate cases of non-compliance
- Communicate with and educate personnel regarding the confidentiality, integrity, and availability of information, information systems, and relevant InfoSec policies and guidelines
- Cascade State security-related messages to Agency senior leadership or personnel

Position Description

- Serve as a primary interface within the Agency for security-related matters; provide input and feedback to Agency leadership regarding policy making, procedures and exceptions pertaining to security requirements impacting the Agency

Back to Overview of InfoSec and Privacy Roles

Role Definition and Responsibility Statements

The following includes initial Position Description language associated with the Privacy Liaison role that could be incorporated into existing job documentation to ensure consistency while supporting compliance across the State.

Privacy Liaison

Role Definition

- Privacy Liaisons serve as a point of contact between State and Agency leadership on activities related to the development, implementation and adherence to Privacy policies and procedures. They may hold a management role in technical areas (e.g., data protection/privacy). This role reports up through the Agency to the Agency Director and/or the Agency Privacy Officer

Role Responsibilities

- Facilitate collaboration between State (e.g., DIS, Enterprise Privacy Office) and Agency personnel, and senior leadership (e.g., Agency Privacy Officer) to plan and execute all Privacy-related efforts, including resolution of Privacy issues within the Agency
- Recognize and address Agency needs for appropriate protection and management of protected data (e.g., Personally Identifiable Information)
- Develop and execute measures to protect data from misuse, unauthorized access or disclosure, loss, alteration, or destruction that may compromise existing Privacy policy and standards
- Initiate, facilitate, and promote activities to foster privacy awareness and adherence to Privacy policies, guidelines and practices (e.g., Privacy training)
- Cascade State Privacy-related messages to Agency senior leadership or personnel

Position Description

- Oversee ongoing activities related to the development, implementation and maintenance of the Agency's Privacy practices in accordance with State Privacy procedures and legal requirements

Back to Overview of InfoSec and Privacy Roles

State of South Carolina Data Classification Schema

The following chart provides an overview of the State's Data Classification criteria.

Public	Data classified as "Public" is intended and/or required for sharing with the public. Examples of public information include but are not limited to: • Information provided on public facing State web sites • Information for public distribution (e.g. state budget after public release)
Internal Use	Data classified as "Internal Use" is non-sensitive information that is used in daily operations of an Agency. If internal use information is inappropriately altered, or is subject to unauthorized access, use or disclosure; little or no loss or harm would be incurred. Examples of internal use information include but are not limited to: • Work phone numbers • Organizational charts • Policies, procedures, and standards
Confidential	Data classified as "Confidential" is sensitive information used by the Agency. If confidential information is inappropriately altered, or is subject to unauthorized access, use or disclosure, considerable loss or harm could occur. Examples of confidential information include but are not limited to: • Unpublished information about agency personnel such as home telephone numbers and home addresses used for emergency contact • Passwords • Security plans, network architecture, etc.
Restricted	Data classified as "Restricted" is highly sensitive information used by the Agency. If restricted information is inappropriately altered, or is subject to unauthorized access, use or disclosure, significant loss including statutory penalties are probable. Examples of restricted information may include but are not limited to: • Federal Tax Information (FTI) received from, or derived from the IRS or secondary sources (IRS Publication 1075) • Student education records (Family Education Right and Privacy Act (FERPA)) • Debit and credit card numbers • Social Security numbers • Protected Health Information (PHI) as defined under HIPAA

Go back to Overview of InfoSec and Privacy Roles