State of South Carolina – Human Resources Division

InfoSec / Privacy Workforce Professional Development Handbook

Table of Contents

1 Introduction

1.1 OVERVIEW

This document provides guidance to the agencies participating in the Information Security (InfoSec) and Privacy Professional Development Program (PDP). The purpose of this program is to support the State of South Carolina's (State) development of an InfoSec and Privacy workforce that is prepared to anticipate and address InfoSec and Privacy risks and threats, with the goal of securing the State's information assets and protecting its citizens.

The purpose of this document is to highlight components of the InfoSec and Privacy PDP and demonstrate the use and reference to PDP artifacts in the hiring, onboarding, training, and performance evaluation of the InfoSec and Privacy workforce.

For further details, please contact the Professional Development Program Manager or your HR Consultant.

1.2 TARGET AUDIENCE

The intended audience for this document includes HR Directors, HR Consultants, Training Coordinators, and other relevant agency stakeholders that are interested in the professional development of the State's InfoSec and Privacy workforce.

1.3 HOW THIS DOCUMENT IS ORGANIZED

This handbook consists of four main sections, which include:

- Hiring
- Onboarding
- Continual Learning and Performance Evaluation
- Frequently Asked Questions (FAQs)

Each of these sections contains subgroups to provide additional details about the InfoSec and Privacy PDP artifacts available for use.

A glossary with common abbreviations can be found in Section 7 of this document.

2 Hiring

2.1 ABOUT THIS SECTION

A major goal of the PDP is to increase the State's InfoSec and Privacy workforce preparedness when anticipating and addressing InfoSec and Privacy risks and threats. The artifacts will help guide agency HR through screening and selecting well-qualified InfoSec and Privacy candidates.

The PDP will assist with hiring through the following three artifacts:

- Roles and Responsibilities
- Position Descriptions (PDs)
- Technical Interview Questions

The following sections include additional detail for each artifact.

2.2 ROLES AND RESPONSIBILITIES

Consistent and clearly defined roles and responsibilities help create employee accountability and ownership, and in turn help increase InfoSec and privacy compliance and competency. The Roles and Responsibilities toolkit helps agencies define roles and responsibilities needed to help support execution of and compliance with State InfoSec and Privacy programs.

Within the toolkit, you will find:

- An overview of the InfoSec and Privacy roles, definitions, and responsibilities that may help agencies understand the roles they need to adopt. The overview also allows State personnel that perform these roles to understand expectations, uphold compliance, and fulfill their role in promoting the State's InfoSec and privacy posture
- A tier categorization that may be used as a guide to determine the minimum number of Full-Time Equivalents (FTEs) needed to fill these roles
- Guidelines for applying roles within agencies
- Role scenarios to illustrate various ways an agency can implement the roles and responsibilities
- A role-to-position map to help illustrate how existing agency positions may fill InfoSec and Privacy roles. Please note that mapping roles to positions will vary by agency. This map is not inclusive of all possible scenarios, rather it serves as an example of how various positions may align to necessary InfoSec and Privacy roles and responsibilities

2.3 POSITION DESCRIPTIONS

The Division of Information Security (DIS), Enterprise Privacy Office (EPO), and Division of State Human Resources (DSHR) have identified 12 unique positions (both new and existing) that can perform the roles and responsibilities necessary to support InfoSec and privacy for the State. These PDs include both Hybrid and Core InfoSec and Privacy positions.

Hybrid positions consist of both InfoSec or Privacy and non-InfoSec or Privacy roles and responsibilities. This is the most common type of position that exists across the State to handle current InfoSec and Privacy responsibilities. The PDs for each position will help formalize and standardize expectations for new and existing staff. Examples of such positions include:

- Information Technology Director
- Network Administrator
- Program Manager – Privacy
- Program Manager – Security

Positions dedicated full-time to InfoSec and/or Privacy roles are Core positions. These individuals will be responsible for various aspects of InfoSec and Privacy programs, processes, and technologies. Examples of such positions include:

- InfoSec Analyst
- Privacy Analyst
- InfoSec and Privacy Auditor
- InfoSec Manager / Chief Information Security Officer (CISO)
- Privacy Manager / Agency Privacy Officer (APO)
- Governance, Risk, and Compliance Manager (GRC)

PDs support the hiring, performance management, and retention of personnel, where appropriate. PDs include position requirements; knowledge, skills, and abilities (KSAs); reporting structure; and job purpose and functions.

2.4 TECHNICAL INTERVIEW QUESTIONS

InfoSec and Privacy Technical Interview Questions help support the hiring of Core personnel, where appropriate. The State has not created Technical Interview Questions for Hybrid positions; please continue using your existing questions for Hybrid job candidates.

These questions are appropriate to use when interviewing for Core InfoSec and Privacy positions, and take into account position-related KSAs, education, professional certification(s), and experience.

3 Onboarding

3.1 ABOUT THIS SECTION

Although the hiring of well-qualified staff is the first step in supporting the State's InfoSec and Privacy workforce, proper onboarding of personnel is equally essential. Agencies are responsible for onboarding newly hired employees and setting appropriate expectations for their roles. This includes defining a clear career path, highlighting training opportunities, and identifying competencies essential to career progression.

The PDP provides the following artifacts to help agencies onboard newly hired or transferred employees:

- Career Path Model
- Competency Model

The following sections include additional detail for each artifact.

3.2 CAREER PATH MODEL

This Career Path Model helps define various career options available to the State's InfoSec and Privacy workforce. The model informs InfoSec and Privacy workforce development planning, evaluations of personnel strengths and areas for improvement, and career progression conversations between supervisors and employees.

The Career Path Model illustrates both Core and Hybrid positions, and potential mobility between each. Career level determination in Hybrid to Core position transfers will be handled on a case-by-case basis with consideration to experience, training, competency-level, and current agency's needs. Some agencies may not have a need for InfoSec or Privacy roles beyond existing positions. Transfers to different agencies may be necessary for InfoSec and Privacy career progression. The Career Path Model specifically includes:

- An overview of the InfoSec and Privacy career path that includes both Technical and Management positions
- An outline of the Technical and Management career paths and possible moves between them
- An overview of competencies and trainings associated with each InfoSec and Privacy position

3.3 COMPETENCY MODEL

The Competency Model outlines requisite KSAs needed to fulfill the State's InfoSec and Privacy positions. The model can serve as a guide for HR and Agency leadership and InfoSec and Privacy personnel alike to:

- Establish proficiency levels for employee success within specific InfoSec and Privacy domains and competencies. These domains and competencies can be referenced by both Core and Hybrid personnel
- Further enhance State HR or talent practices such as individual learning plans

- Help InfoSec and Privacy employees manage their own careers by providing them with a clear understanding of expected KSAs for each InfoSec and Privacy domain

4 Continual Learning & Performance Evaluations

4.1 ABOUT THIS SECTION

As State agency needs evolve due to ever-changing InfoSec and Privacy threats, State employees should strive to strengthen their respective KSAs. Continual learning helps employees adapt to new threats, progress in their career, and better serve the needs of the State. Supervisors may also use learning requirements to support workforce performance evaluations, identify new training opportunities and make decisions for future workforce planning.

The PDP provides the following artifacts to help agencies evaluate employee performance and identify training opportunities to strengthen their Core and Hybrid InfoSec and Privacy workforce:

- Training Framework
- Competency Model
- PDs

The following sections include additional detail for each artifact.

4.2 TRAINING FRAMEWORK

The Training Framework provides a catalog of courses for both Core and Hybrid InfoSec and Privacy positions. Clearly defined courses and professional certifications help encourage growth and ownership of InfoSec and Privacy domains at each State agency, and in turn increase InfoSec and privacy compliance and competency.

InfoSec and Privacy leadership and staff can use the framework in a variety of ways to support their own and their team’s professional development and career growth. Personnel can search for training opportunities by:

- PDs
- Competency
- Certification

4.3 COMPETENCY MODEL

The Competency Model described in Section 3.2 of this document can also provide guidance for continual training and performance evaluation of Core and Hybrid InfoSec and Privacy employees. The model specifically:

- Outlines knowledge needed to fulfill various InfoSec and Privacy roles
- Establishes proficiency levels for employee success within specific InfoSec and Privacy domains and competencies
- Provides agencies with a framework to perform skills assessments and determine which InfoSec and Privacy workforce domains need additional training or workforce planning investments
- Further enhances State HR and talent practices, including training curriculum development and evaluation of employee performance

4.4 POSITION DESCRIPTIONS

The PDs described in Section 2.3 of this document can also provide guidance for continual training and performance evaluation of Core and Hybrid InfoSec and Privacy employees. The PDs outline position requirements, KSAs, job purpose, and job functions for career progression and evaluation of employee performance. Evolving InfoSec and Privacy demands may necessitate changes to the Core and Hybrid PDs, corresponding continual learning opportunities and performance evaluations.

5 FAQs

5.1 ABOUT THIS SECTION

The FAQ document captures frequently asked questions about the InfoSec and Privacy PDP artifacts and deployment.

The FAQ document follows a similar layout to this handbook, allowing for ease of use and understanding. The FAQs address hiring, onboarding, continual learning and performance evaluation questions as they pertain to the InfoSec and Privacy workforce.

6 Summary

The purpose of the InfoSec and Privacy PDP is to help the State develop an InfoSec and Privacy workforce that is prepared to address InfoSec and Privacy risks and threats, with the goal of securing the State's information assets and protecting its citizens.

The PDP artifacts described above, along with this Handbook, serve as a guide to help develop the State's InfoSec and Privacy workforce. These artifacts specifically support the hiring, onboarding, continuous learning, and performance evaluation of InfoSec and Privacy employees.

As the needs of State agencies evolve due to ever-changing InfoSec and Privacy threats, these artifacts should be reviewed and modified accordingly. Should you need copies of these artifacts or have additional questions related to the InfoSec and Privacy PDP, please contact the Professional Development Program Manager or your HR Consultant.

7 Glossary

Full Form	Abbreviation
Agency Privacy Officer	APO
Chief Information Security Officer	CISO
Division of Information Security	DIS
Enterprise Privacy Office	EPO
Governance, Risk, and Compliance	GRC
Information Security	InfoSec
Knowledge, Skills, and Abilities	KSAs
Frequently Asked Questions	FAQs
Full-Time Equivalent	FTE
Position Description	PD
Professional Development Program	PDP
State of South Carolina	State

8 Appendix[1]

8.1 ROLES AND RESPONSIBILITIES TOOLKIT

Reference document SC PDP Roles and Responsibilities - For more information or questions related to the InfoSec and Privacy PDP, please contact the Professional Development Program Manager or your HR Consultant.

8.2 COMPETENCY MODEL

Reference document SC PDP Competency Model - For more information or questions related to the InfoSec and Privacy PDP, please contact the Professional Development Program Manager or your HR Consultant.

8.3 POSITION DESCRIPTIONS

Reference document SC PDP Position Descriptions - For more information or questions related to the InfoSec and Privacy PDP, please contact the Professional Development Program Manager or your HR Consultant.

8.4 TECHNICAL INTERVIEW QUESTIONS

Reference document SC PDP Technical Questions - For more information or questions related to the InfoSec and Privacy PDP, please contact the Professional Development Program Manager or your HR Consultant.

8.5 TRAINING FRAMEWORK

Reference document SC PDP Training Framework - For more information or questions related to the InfoSec and Privacy PDP, please contact the Professional Development Program Manager or your HR Consultant.

8.6 CAREER PATH MODEL

Reference document SC PDP Career Path Model - For more information or questions related to the InfoSec and Privacy PDP, please contact the Professional Development Program Manager or your HR Consultant.

8.7 FAQS

Reference document SC PDP FAQS - For more information or questions related to the InfoSec and Privacy PDP, please contact the Professional Development Program Manager or your HR Consultant.

[1] Reference to these artifacts were last updated August 20thth, 2015 and are subject to change. Please refer to the DSHR website or contact the Professional Development Program Manager at DSHR for the latest versions.