# State of South Carolina Policy Guidance Initiative

## Roles and Responsibilities Chart

## [AGENCY NAME]

|  |  |
| --- | --- |
| **Agency Teams** | **Responsibilities** |
| Policy Champion | * Individual with a management role in the areas of compliance, information security (InfoSec) and/or technology
* Lead the information security policy implementation effort for the Agency
* Identify and coordinate with Policy Deployment Teams
* Liaison between Agency senior leadership team (i.e. Agency Director) and Policy Deployment Team(s)
 |
| Policy Deployment Team(s) | * Collection and review of relevant information securities policies, standards and processes
* Conduct a gap analysis and document a policy implementation plan
* Identifying and resolving policy deployment challenges and risks
* Develop a policy implementation roadmap
* Coordinate with Policy Champion on policy implementation activities
 |

|  |  |
| --- | --- |
| **Policy Champion** | **[AGENCY POLICY CHAMPION]** |
| **State of South Carolina****Information Security Policies** | **Policy Sections** | **Policy Deployment Team** | **Implementation Role(s)** | **Implementation Responsibilities** | **Revision and** **Approval**  |
| (e.g., HR Team, Software Developer, ‘Bob Smith’, etc.) | (e.g., document the implementation plan, identify and implement remediation strategies, etc.) | (i.e., key stakeholders to review and sign off policies)  |
| Access Control | Access Management |  |  |  |  |
| Network Access Management |  |  |  |  |
| Identity Management |  |  |  |  |
| Authentication |  |  |  |  |
| Emergency Access |  |  |  |  |
| Password Policy |  |  |  |  |
| Password Administration |  |  |  |  |
| Asset Management | Asset Identification |  |  |  |  |
| Business Continuity Management  | Contingency Planning |  |  |  |  |
| Disaster Recovery and Contingency Strategies |  |  |  |  |
| Data Backups |  |  |  |  |
| Data Privacy & Protection | Data Classification |  |  |  |  |
| Data Disposal |  |  |  |  |
| Data Protection |  |  |  |  |
| Privacy |  |  |  |  |
| HR & Security Awareness | Human Resource Compliance |  |  |  |  |
| Security Awareness Training |  |  |  |  |
| IT Compliance | Audit and Compliance Requirements |  |  |  |  |
| Information System Audit Considerations |  |  |  |  |
| Review, Monitoring and Response Program |  |  |  |  |
| IT Risk Strategy | Enterprise Architecture Security |  |  |  |  |
| Security Performance and Metrics |  |  |  |  |
| Third Party Risk Management |  |  |  |  |
| Information System Acquisition, Development & Maintenance | Change Management |  |  |  |  |
| Configuration Management |  |  |  |  |
| System Development and Maintenance |  |  |  |  |
| Release Management |  |  |  |  |
| Master Policy | Information Security Program Planning |  |  |  |  |
| Security Organization (Roles and Responsibilities) |  |  |  |  |
| Policy Management (Plan of Action) |  |  |  |  |
| Information Security Controls Deployment |  |  |  |  |
| Mobile Security  | Mobile Security |  |  |  |  |
| Removable Media Security |  |  |  |  |
| Laptop Security |  |  |  |  |
| Physical & Environmental Security | Physical Access and Security |  |  |  |  |
| Environmental Security |  |  |  |  |
| Disposal of Equipment |  |  |  |  |
| Risk Management | Risk Management |  |  |  |  |
| Risk Assessment |  |  |  |  |
| Risk Mitigation |  |  |  |  |
| Threat & Vulnerability Management | Vulnerability Assessment |  |  |  |  |
| Incident Management |  |  |  |  |
| Patch Management |  |  |  |  |