



Clarifying Roles

Last Updated: August 2025

DISCLAIMER

The information in this document is provided as a resource to assist governmental entities and does not constitute legal advice. Your level of responsibility for the duties described may range from being directly accountable to simply being informed or consulted. Be sure to involve legal counsel where appropriate.

Job Duties

DATA PRIVACY

Primary Focus: Ensuring compliance with data protection laws and promoting a privacy conscious culture.

Common Duties:

- Create and maintain notices for all government websites.
- Provide data collection notices.
- Ensure the entity is only obtaining and processing the minimum amount of personal data necessary to achieve a specific purpose.
- Assure all data sharing and disclosure practices comply with applicable legal authority.
- Monitor data processing activities for compliance with privacy laws and internal data protection policies (e.g., GDPR, HIPAA, state specific acts).
- Advise leadership and staff on privacy and data protection obligations.
- Conduct privacy impact assessments (PIAs) and risk assessments.
- Develop and maintain privacy policies, procedures, and documentation.
- Oversee training and awareness programs for employees on data privacy principles and practices.
- Serve as a point of contact for data subjects regarding privacy related inquiries and rights requests (e.g., access, correction, deletion).
- Coordinate responses to data breaches, including investigation, mitigation, notification, and documentation.
- Liaise with regulatory authorities and ensure proper reporting of privacy incidents.
- Evaluate contracts and third-party agreements for data privacy risks and compliance.
- Stay current with evolving privacy regulations and industry standards to advise on necessary changes or improvements.
- Promote a privacy first culture across the organization through collaboration and advocacy.

RECORDS MANAGEMENT

Primary Focus: Managing the lifecycle of records in compliance with legal and regulatory requirements.

Common Duties:

- Oversee the creation, designation, classification, and indexing of record series to ensure accurate organization and efficient retrieval.
- Draft, propose, and implement records retention schedules in alignment with legal, regulatory, privacy, and operational requirements.
- Ensure the lawful, timely, and secure disposition or destruction of obsolete records, including those containing personal data, to support compliance, efficiency, and responsible data stewardship.
- Train staff in records handling procedures, retention requirements, and documentation standards.
- Fulfill annual Records Officer training and certification through DARS.
- Process records requests and ensure timely, lawful responses to each one.
- Coordinate records transfers and archiving with state archives or designated repositories.
- Advise departments on document management systems and best practices for file naming, version control, and storage formats.
- Assess records practice to ensure compliance with records retention laws and policies.
- Maintain inventories of records and track records in active and inactive use.
- Facilitate continuity of operations planning (COOP) by ensuring critical records are accessible during emergencies.

CYBERSECURITY

Primary Focus: Protecting digital systems, networks, and data from unauthorized access, attacks, and vulnerabilities.

Common Duties:

- Protect networks, systems, and data from unauthorized access, breaches, and cyberattack.
- Implement and manage security controls such as firewalls, antivirus software, intrusion detection systems, and endpoint protection.
- Monitor networks and systems for security breaches or suspicious activity.
- Respond to security incidents through alerts, forensic analysis, and remediation.
- Perform vulnerability assessments and penetration testing to identify and reduce risk.
- Develop and enforce security policies and procedures aligned with industry standards (e.g., NIST, ISO 27001).
- Manage user access controls and authentication protocols to enforce least privilege principles.
- Provide training and awareness programs on secure practices (e.g. phishing prevention).
- Encrypt sensitive data and ensure secure data transmission and storage.
- Conduct regular security audits and risk assessments, including vendor/system evaluations.
- Educate staff on cybersecurity awareness (e.g., phishing, strong passwords, threat avoidance).
- Collaborate with IT, legal, and privacy teams to align security practices with compliance needs.