AUBURN
Human Resources

Privacy Program Manager

Job Description

JOB INFORMATION

Job Code	KC28
Job Description Title	Privacy Program Manager
Pay Grade	LC12
Range Minimum	$76,560
33rd %	$96,970
Range Midpoint	$107,180
67th %	$117,390
Range Maximum	$137,800
Exemption Status	Exempt
Organizational use restricted to the following divisions	101 VP InstitutionalCompliance&Security
Approved Date:	4/27/2026 4:15:18 PM

JOB FAMILY AND FUNCTION

Job Family:	Legal, Compliance & Audit
Job Function:	Risk Management

JOB SUMMARY

Oversees the management, coordination, and assessment of the University's data-privacy activities, directing the University-wide privacy program in alignment with federal, state, and international privacy requirements and serves as Auburn University's HIPAA Privacy Officer. Collaborates with decentralized privacy functions to strengthen institutional privacy strategy, policies, best practices, and contractual safeguards; plans and delivers training programs; consults with departments to enhance internal processes and reduce risks associated with data-privacy incidents; and promotes a strong culture of data stewardship, accountability, and ethical compliance across the University.

RESPONSIBILITIES

- Supports the design, implementation, and ongoing maintenance of the University’s data-privacy program, including policies, procedures, standards, and operational controls that protect personal and sensitive information across academic and administrative functions. Provides guidance on the development, implementation, and maintenance of University-wide privacy policies and procedures. Manages data-breach notification assessments and response activities in accordance with applicable state, federal, and international privacy laws. Reviews software and third-party vendor requests to ensure compliance with University data-privacy requirements and to confirm that contractual terms adequately safeguard University data and minimize institutional risk.
- Manages all activities related to the development, implementation, and maintenance of Auburn’s HIPAA privacy program, including policies, procedures, and core documentation governing the confidentiality and protection of PHI. Conducts and documents recurring training for units with access to ePHI, audits Business Associate Agreements and related workflows, and ensures compliance with HIPAA, the HITECH Act, and applicable state laws.
- Supports administration of the University’s Electronic Privacy Policy by providing e-discovery and electronic-preservation services to the Office of General Counsel, Division of Internal Audit, Research Integrity and Compliance, Athletics Compliance, and external counsel, in accordance with University policy and the Office of Audit, Compliance & Privacy Charter. Provides subject-matter expertise to the Office of General Counsel regarding the sequestering, securing, or preservation of data in response to litigation, subpoenas, investigations, and public-records requests.
- Serves as a resource to academic and administrative units by consulting on, evaluating, and remediating issues related to the confidentiality and protection of University records in both electronic and physical formats. Collaborates with stakeholders across the institution to support data-governance best practices, including appropriate data retention and deletion. Cultivates strong relationships with campus partners to strengthen the University’s culture of compliance, ethics, and shared accountability. Provides clear, practical guidance consistent with applicable laws, regulations, and University policies.

RESPONSIBILITIES

- Maintains current knowledge of federal, state, and international privacy laws and regulations, including FERPA, HIPAA, GLBA, CCPA, GDPR, and other emerging privacy frameworks. Provides guidance to University stakeholders to ensure institutional compliance with evolving legal and regulatory requirements.
- Monitors organization-wide compliance with privacy laws and University policies, conducting audits to identify, document, and remediate compliance gaps. Evaluates whether required training, documentation, and operational processes are being maintained effectively and efficiently. Delivers data-privacy training as needed and recommends corrective actions to support adherence to privacy laws and to strengthen the University's overall compliance program in alignment with the U.S. Federal Sentencing Guidelines.

The responsibilities listed above show the typical duties for jobs in this classification. Actual tasks may differ depending on the department's needs. Other similar duties may be assigned with discretion of the supervisor. Not every duty will apply to every position, and the amount of time spent on each task can change based on department needs.

SUPERVISORY RESPONSIBILITIES

Supervisory Responsibility	May supervise employees but supervision is not the main focus of the job.

MINIMUM QUALIFICATIONS

To be eligible, an individual must meet all minimum requirements which are representative of the knowledge, skills, and abilities typically expected to be successful in the role. For education and experience, minimum requirements are listed on the top row below. If substitutions are available, they will be listed on subsequent rows and may only to be utilized when the candidate does not meet the minimum requirements.

MINIMUM EDUCATION & EXPERIENCE

Education Level	Focus of Education		Years of Experience	Focus of Experience	
Bachelor's Degree	Business, Law, Communication, Public Administration, or related field.	and	5 years of	experience in privacy law, regulatory compliance, healthcare management, HIPAA, GDPR, research administration, auditing, legal services, organizational compliance, or a related field. Experience in a higher-education environment—particularly interpreting and applying laws and regulations—is preferred.	

MINIMUM KNOWLEDGE, SKILLS, & ABILITIES

Strong knowledge of federal and state privacy laws and regulations	
Demonstrated understanding of data-integrity, privacy practices, and risk/compliance management frameworks	
Knowledge of privacy-program development and governance	
Strong analytical and investigative skills	
Exceptional communication and training abilities	
Ability to build collaborative relationships across decentralized units	
Ability to manage and safeguard sensitive information	

MINIMUM LICENSES & CERTIFICATIONS

Licenses/Certifications	Licenses/Certification Details	Time Frame	Required/ Desired	
	Certified Compliance & Ethics Professional (CCEP)	Upon Hire	Required	Or
	Certified Information Privacy Professional (CIPP)/US	Upon Hire	Required	Or

MINIMUM LICENSES & CERTIFICATIONS

Licenses/Certifications	Licenses/Certification Details	Time Frame	Required/ Desired	
	Certified Information Privacy Manager (CIPM)	Upon Hire	Required	Or

PHYSICAL DEMANDS & WORKING CONDITIONS

Physical Demands Category:	Other

PHYSICAL DEMANDS

Physical Demand	Never	Rarely	Occasionally	Frequently	Constantly	Weight
Standing			X			
Walking			X			
Sitting				X		
Lifting		X				25 lbs
Climbing			X			
Stooping/ Kneeling/ Crouching			X			
Reaching			X			
Talking					X	
Hearing					X	
Repetitive Motions				X		
Eye/Hand/Foot Coordination				X		

WORKING ENVIRONMENT

Working Condition	Never	Rarely	Occasionally	Frequently	Constantly
Extreme cold		X			
Extreme heat		X			
Humidity			X		
Wet		X			
Noise			X		
Hazards		X			
Temperature Change			X		
Atmospheric Conditions		X			
Vibration		X			

Vision Requirements:

Ability to see information in print and/or electronically.