COURSE SYLLABUS

Data Protection & Privacy Certificate Program (Self-Paced)

Covers the rules that govern sensitive information in federal work: protecting PII and PHI under the Privacy Act, recognizing and marking CUI, and managing federal records from creation through lawful disposition.

> Group classes (Live Online) and onsite training are available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/certificates/data-protection-privacy-certificate-self-paced



support@graduateschool.edu •
(888) 744-4723

Course Outline

This package includes these courses

- Privacy and PII/PHI Protection Awareness Course (Self-Paced) (4 hours)
- CUI Handling and Data Classification Course (Self-Paced) (4 hours)
- Records and Information Governance Course (Self-Paced) (6 Hours)

Privacy and PII/PHI Protection Awareness Course (Self-Paced)

A foundational, agency-neutral privacy course spanning the Privacy Act, PII and PHI identification, safeguarding requirements, and the federal breach-response lifecycle.

- The purpose and key requirements of the Privacy Act of 1974 and related federal privacy guidance
- Defining and identifying PII and PHI across federal work contexts
- The Fair Information Practice Principles applied to everyday activities
- Administrative, physical, and technical safeguards for sensitive information
- The steps to report and respond to a suspected or confirmed privacy incident
- Individual roles and responsibilities in a culture of privacy protection

CUI Handling and Data Classification Course (Self-Paced)

Agency-neutral awareness training across the CUI lifecycle — recognition, categories, marking, handling, destruction, incident reporting, and CUI with AI tools.

- CUI defined, and how it differs from classified and from public information
- The government-wide legal and regulatory framework for CUI
- CUI Basic versus CUI Specified, and checking a category in the CUI Registry

- Interpreting and assembling banner markings, and portion marking
- Need-to-know and safe handling in physical, electronic, and verbal forms
- Approved storage, transmission, destruction, and sanitization
- Responding when CUI is lost, mishandled, or improperly disclosed
- Government-wide expectations for using CUI with AI tools

Records and Information Governance Course (Self-Paced)

Intermediate federal recordkeeping covering what counts as a record, the records lifecycle, retention and disposition scheduling, and electronic records in email, chat and collaboration platforms.

- A federal record defined and separated from non-record material, convenience copies, drafts and personal papers
- The legal and policy basis for federal recordkeeping, and who does what up to NARA
- Each stage of the records lifecycle and individual responsibilities at each
- Adequate and proper documentation, and common recordkeeping failures
- Litigation holds and the duty not to alter or delete
- Why an unscheduled record cannot be destroyed, and how General Records Schedules work
- Temporary versus permanent records and end-of-retention outcomes
- Reporting obligations after unauthorized or accidental destruction
- Email, chat and collaboration messages as federal records
- Metadata and electronic recordkeeping practice
- Where records governance meets privacy, FOIA and CUI
- Recurring compliance activities and escalation paths