

UTEP Standard 26: Internally Developed Application Security and Governance

- 26.1 Introduction. The University of Texas at El Paso (“UTEP” or “University”) recognizes that internally developed applications are critical components supporting the University’s academic, research, administrative, healthcare, and public service missions. These applications may process, store, transmit, or provide access to University Data, including controlled, confidential, or Controlled Unclassified Information (CUI).

Internally developed applications may be created by centralized or decentralized IT organizations, academic departments, research groups, administrative units, contractors, or individual developers operating on behalf of the University. Because these applications introduce operational, security, compliance, and data protection risks, the University establishes minimum governance and security requirements for their development, deployment, operation, and maintenance.

- 26.2 Purpose. It is the purpose of this Standard to:
- (a) establish minimum governance and security requirements for internally developed applications;
 - (b) ensure that applications processing University Data are appropriately identified, classified, and managed;
 - (c) reduce risks associated with unauthorized access, disclosure, modification, destruction, or misuse of University Data;
 - (d) establish requirements for secure development, deployment, maintenance, and decommissioning of internally developed applications;
 - (e) ensure the Information Security Office is notified when applications collect, process, transmit, store, or provide access to controlled, confidential, or Controlled Unclassified Information (CUI);
 - (f) establish accountability for ownership and management of internally developed applications; and
 - (g) support compliance with applicable federal and state laws, regulations, contractual obligations, and University policies.
- 26.3 Applicability. This Standard applies to:
- (a) all internally developed applications owned, operated, managed, hosted, or maintained by the University or on behalf of the University;
 - (b) all internally developed applications developed by centralized IT, decentralized IT, academic departments, research programs,

contractors, student organizations acting on behalf of the University, or third parties operating for University business purposes;

- (c) all internally developed applications regardless of:
 - i. programming language,
 - ii. hosting environment,
 - iii. platform
 - iv. infrastructure type,
 - v. or deployment model;
- (d) applications hosted:
 - i. on-premises,
 - ii. in cloud environments,
 - iii. externally hosted,
 - iv. or within third-party services;
- (e) applications classified as web applications, desktop applications, mobile applications, scripts, APIs, databases, low-code/no-code solutions, automation tools, artificial intelligence systems, or research-developed systems; and
- (f) all individuals responsible for developing, managing, administering, supporting, or using internally developed applications.

26.4 Policy Statement. All internally developed applications shall be developed, deployed, maintained, and operated in accordance with University Information Security Policies, Standards, Procedures, and applicable legal and regulatory requirements.

Application owners and developers are responsible for ensuring that appropriate security controls are implemented based on the classification and risk level of the data processed by the application.

Applications processing controlled, confidential, or Controlled Unclassified Information (CUI) shall be subject to review by the Information Security Office prior to production deployment.

26.5 Application Registration and Inventory

- 26.5.1 All internally developed applications shall be registered with the University prior to production deployment.
- 26.5.2 Registration shall include, at a minimum:
 - (a) application name;
 - (b) business purpose;
 - (c) application owner;

- (d) technical support contact;
- (e) hosting location;
- (f) authentication method;
- (g) data classification;
- (h) whether the application is externally accessible;
- (i) integration with third-party services;
- (j) whether the application stores, processes, transmits, or provides access to controlled, confidential, or Controlled Unclassified Information (CUI);
- (k) whether the application utilizes artificial intelligence or automated decision-making processes; and
- (l) whether the application integrates with institutional authentication, identity, or enterprise systems.

26.6 Data Classification and Security Review

26.6.1 Application owners and developers shall classify data processed by the application in accordance with the UTEP Data Classification Standard.

26.6.2 The Information Security Office must be notified prior to production deployment when an application:

- (a) stores, processes, transmits, or provides access to controlled, confidential, or Controlled Unclassified Information (CUI);
- (b) integrates with institutional authentication systems;
- (c) is accessible from the internet;
- (d) processes financial, student, employee, healthcare, research, or controlled information;
- (e) uses cloud-hosted infrastructure or third-party hosted services;
- (f) utilizes artificial intelligence systems or automated processing involving University Data; or

26.6.3 The Information Security Office may require:

- (a) architecture review;
- (b) vulnerability assessment;
- (c) penetration testing;
- (d) remediation of identified vulnerabilities;
- (e) logging and monitoring controls;
- (f) encryption requirements;

- (g) documentation of data flows and integrations; or
- (h) additional safeguards based on institutional risk.

26.7 Minimum Security Requirements. Internally developed applications shall implement security controls appropriate to the classification and risk level of the application and associated data.

At minimum, applications shall:

- (a) implement authentication and authorization controls appropriate to the application's purpose and risk;
- (b) use encrypted communications protocols for transmission of confidential or controlled data;
- (c) protect sensitive data at rest where applicable;
- (d) follow secure coding practices designed to reduce common application vulnerabilities;
- (e) validate user input and protect against injection and unauthorized execution attacks;
- (f) maintain logging appropriate for security monitoring, auditing, and incident response;
- (g) maintain current supported software components, frameworks, and dependencies;
- (h) remediate known critical vulnerabilities within timelines established by the Information Security Office;
- (i) restrict privileged access to authorized personnel;
- (j) support backup and recovery capabilities appropriate to institutional operations;
- (k) separate development, testing, and production environments where feasible; and
- (l) restrict the use of production data within development or testing environments unless appropriately authorized and protected.

26.8 Change Management and Maintenance

26.8.1 Internally developed applications shall follow established University change management processes where applicable.

26.8.2 Application owners shall ensure applications are maintained throughout their operational lifecycle, including:

- (a) security updates;
- (b) business purpose;
- (c) dependency and framework updates;

- (d) access reviews;
 - (e) logging and monitoring reviews; and
 - (f) retirement or decommissioning processes.
- 26.8.3 Unsupported, abandoned, or unmaintained applications that present elevated institutional risk may be restricted, isolated, removed from operation, or denied access to University Information Resources.
- 26.9 Roles and Responsibilities
 - 26.9.1 Application Owner. The Application Owner is responsible for:
 - (a) ensuring compliance with this Standard;
 - (b) classifying application data;
 - (c) coordinating required security reviews;
 - (d) ensuring ongoing maintenance and support;
 - (e) authorizing user access where applicable;
 - (f) ensuring appropriate safeguards are implemented; and
 - (g) ensuring unsupported or unnecessary applications are decommissioned appropriately.
 - 26.9.2 Developers. Developers are responsible for:
 - (a) following secure development practices;
 - (b) protecting University Data during development and testing;
 - (c) remediating identified vulnerabilities;
 - (d) notifying the Information Security Office of applications processing confidential or controlled data;
 - (e) complying with applicable University security requirements; and
 - (f) maintaining documentation sufficient to support operational continuity and security review processes.
 - 26.9.3 Information Security Office. The Information Security Office is responsible for:
 - (a) defining security requirements and guidance;
 - (b) conducting security reviews and assessments;
 - (c) assisting departments with risk evaluations;
 - (d) identifying institutional security risks associated with internally developed applications;
 - (e) establishing remediation requirements where necessary; and

- (f) developing procedures, guidelines, and supporting standards associated with this Standard.

26.10 Exceptions. Exceptions to this Standard must be formally documented and approved through the University's Information Security exception process.

Compensating controls may be required where full compliance is not technically or operationally feasible.

Documented acceptance of residual risk may be required prior to production deployment.

26.11 Enforcement. Failure to comply with this Standard may result in:

- (a) removal of application access;
- (b) restriction of application functionality;
- (c) disconnection from University Information Resources;
- (d) required remediation activities;
- (e) suspension of production deployment; or
- (f) disciplinary action in accordance with University policies and procedures.

26.12 References

- [U.T. System Policy 165: Information Resources Use and Security Policy](#)
- [University Information Security Office – Policies](#)
- [Texas Administrative Code, Chapter 202: Information Security Standards](#)
- [NIST 800-171: Protecting Controlled Unclassified Information in Nonfederal System and Organizations](#)
- [Payment Card Data Security Standard \(PCI-DSS\)](#)
- [24 CFR Part 99 - Family Educational Rights and Privacy Act](#)
- [H.R.3763 - Sarbanes-Oxley - Act of 2002](#)
- [General Data Protection Regulation \(GDPR\) – Legal Text](#)

26.13 Revision History

First Draft: May 27, 2026

Approved: May 28, 2026

Gerard D. Cochrane Jr., Chief Information Security Officer

26.14 Contact Information. Questions or comments regarding this Standard should be directed to:

security@utep.edu