Web-based Application Standard

Objective

In accordance with the Information Security and Acceptable Use Policy, all web-based applications developed, licensed, and/or operated by UT Dallas must be adequately protected to ensure confidentiality, integrity, availability, and accountability of such systems.

Physical Location

All production web-based applications should be operated on servers in rooms that meet the applicable minimum standards defined in the Standard for Server Rooms.

Support Requirements

All web-based applications developed by a 3rd party must have a valid support contract or, in the case of open-source software, be commercially or community supported. Costs to achieve and maintain appropriate information security must be included in the project's budget.

Patching

Security patches must be tested and installed in a timely manner, depending on the likelihood and impact of vulnerability exploitation.

DNS Naming

When warranted to promote application migration to alternate hardware, applications should be accessed via a DNS alias, rather than the name of the server that hosts the application.

Authentication and Access Control

Built-in accounts, such as administrative accounts, should be disabled if not used and must not have blank or default passwords. Applications that host Confidential or Controlled Data must adequately limit access to view or change that data to individuals requiring such access. All applications, including those which host Public Data, must adequately limit access to change that data to individuals requiring such access. When feasible, Shibboleth federation (also referred to as the Comet Authentication Service) should be used as the authentication mechanism.

Encryption

Transmission of Confidential Data, including authentication credentials, must be performed via an encrypted channel using trusted certificates such as those provided by the Information Security Office via InCommon. Use of self-signed certificates in production environments is not recommended. Confidential Data in transit must be encrypted using a minimum of 128-bit encryption. 256-bit encryption is recommended where feasible.

System Logon Banner

Internet-facing applications that require authentication must be configured to present users with the University logon banner, as follows:

Use of UTD Information Systems is subject to the UTD Information Security and Acceptable Use Policy. Pursuant to Texas Administrative Code 202: (1) Unauthorized use is prohibited; (2) Usage may be subject to security testing and monitoring; (3) Misuse is subject to criminal prosecution; and (4) Users have no expectation of privacy except as otherwise provided by applicable privacy laws.

Automatic Log-off

Applications that require authentication must be configured to automatically end a user's session after a time period consistent with the business purpose of the application. The Information Security Office recommends 20 minutes for applications serving Confidential Data.

Logging

Application activity must be logged and retained for a minimum of 90 days to facilitate troubleshooting and investigations. The following types of activities must be logged:

- Successful and unsuccessful login attempts
- Any application or data modification operation, such as insertion, updates, or deletion of data, changes to application configuration, etc. Logging of read / query activities is required for applications containing HIPAA data and is recommended for other applications when feasible.

Application logs should also be sent to a centralized logging server to reduce storage requirements on local systems, facilitate correlation, and reduce feasibility of log tampering.

Vulnerability Assessment

All applications are subject to periodic application vulnerability scans conducted or sponsored by the Information Security Office. For applications that are Internet-accessible or host Confidential or Controlled Data, these scans must be conducted at least annually. All other applications must be scanned for application vulnerabilities every two years. System owners are responsible for timely remediation of identified vulnerabilities.

Configuration and Access Control

Applications must be developed and maintained with appropriate security controls. Controls must also be documented. Some examples include:

- Unnecessary files, including default templates and directories, should be removed from production systems.
- Directory viewing on web application servers should be disabled.
- Only users tasked with making website updates should be granted write access within web root folders.

- HTML static pages must not have execute permissions.
- Logon or authentication cookies must not be persistent.
- Hostnames, usernames, or database names should not be hardcoded into applications and scripts.
- Back-end servers must verify the identity of requesting web servers.

Administrative Interfaces

For Internet-facing applications, the management or administrative interface should be configured to be accessible only from within the UT Dallas network, or restricted to only allow access by a known list of external IP addresses, when feasible.

Authentication Session Management

Authentication session management protocols will be used in web applications for testing, development, and production environments. Such access controls include, but are not limited to:

- New session IDs are generated for each new login request.
- Session IDs should be random and not sequential in nature.
- Encryption is required to protect authentication of session IDs in transit between servers and clients.
- Session data must not readily identify users or individuals according to existing attributes, such as NetID or UTD-ID.
- All session data must be destroyed when a user logs off.

Data Validation

All input of data, including usernames and passwords, must be verified on the server side of the application. Client-side validation is encouraged but should not be relied upon for validation.

Database Interfaces

When present, database interfaces should be configured to provide adequate security controls. Examples include:

- Storage of database names, usernames, passwords, and hostnames should reside outside of the code base.
- Web applications should use dedicated accounts that are not default database accounts and do not have administrative privileges on such databases.
- Applications must use encryption to access Confidential or Controlled Data on databases located on other systems.

Incident Management

Application owners are required to report any suspicious activity to the Information Security Office for investigation.

Backups

Unless backup functions are configured at the server level, application data must be backed up in an automated fashion consistent with the business requirements for recovery time objective (length of time the system can be offline) and recovery point objective (amount of data at risk since the most recent backup, replication, or other data protection event). Stored backups must also meet security protections comparable to the source server.

Business Continuity Planning / Disaster Recovery

All mission-critical systems must be covered by an applicable Business Continuity Plan (BCP) and Disaster Recovery (DR) plan.

Exemptions

In the event that compliance with this web-based application standard cannot be met, please contact infosecurity@utdallas.edu to submit an exemption request which will be approved or denied by the CISO. Denied exemption requests may be appealed to the UT Dallas President for final decision.