Responsible Executive: Chief Information Officer
Responsible Office: Information Technology Services
Effective Date: June 21, 2005
Last Revised: TBD

WEB APPLICATION SECURITY

POLICY SUMMARY

Common methods for accessing University Information including Web Applications. These computer software programs can be particularly susceptible to computer hacking attacks due to their public visibility and accessibility. This can result in the exposure or modification of University Information. To mitigate these risks, University Community Members responsible for creating, developing, updating, maintaining, or administering University Web Applications are required to implement appropriate classification and security procedures in accordance with this policy and its accompanying Web Application Security Standard.

REASON FOR THIS POLICY

Testing, assessing, and securing Web Applications deployed at the University is an essential element of meeting the University's obligation to maintain the confidentiality, integrity, and availability of University Information and IT Resources.

ENTITIES AFFECTED BY THIS POLICY

- Information Security Services
- Web Application administrators
- Web Application Developers

WHO SHOULD KNOW THIS POLICY

- Chief Information Officer ("CIO")
- Director, Information Security Services (ISS)
- External agents granted access to University Information acting for or on behalf of the University
- System administrators
- University Community Members who manage or are responsible for Web Applications
- Web Application vendors or providers

DEFINITIONS

Authentication Methods: the technical process used to determine the validity or legitimacy of a Digital Identity, updated periodically to reflect best practices in security management. Security methods are approved by the CIO, or their designee, and documented as institutional IT procedures.

Digital Identity: a set of attributes stored as electronic data that represent or describe a person, device, or service. These attributes may include, but are not limited to, a name, an electronic mail address, login credentials, or similar identifying information that when taken together, unmistakably describe and identify the person, device, or service.

Information Technology ("IT") Resource: any computer, server, communication or mobile device, or electronic data, data storage, transmission or control device that is owned and/or operated by the University, used to conduct University business, or connected to the University's IT networking or communication systems regardless of ownership, location, or access method. These resources are referred to herein as "IT Resources."

System Administrators: University employees responsible for configuring, architecting, engineering, administering, and maintaining University IT Resources for use by Authorized Users for authorized purposes.

Threat Modeling: a process to identify, communicate, and understand threats and mitigations within the context of protecting something of value.

University Community Member: all University faculty, staff, student employees, students, alumni, affiliates, contractors, consultants, agents, and volunteers wherever located.

University Information: all written or verbal data or information that the University or its employees, students, or designated affiliates or agents collect, possess, or have access to regardless of the medium on which it is stored or its format.

Web Application: a software program that utilizes a web browser—common examples include Internet Explorer, Chrome, Safari, and Firefox—and other web technology to perform tasks over a network, such as an intranet or the Internet. Common examples of vendor or provider-created Web Applications include the Google G-Suite programs and "Louie," which is a prominent example of a University Web Application. Web Applications are also created, or developed, internally for University business by Web Application developers.

Web Application Administrator: University employees responsible for managing the deployment, maintenance, and overall health of web applications and their associated server infrastructure. These roles may also be called System Administrator or DevOps engineer.

Web Application Developer: University employees responsible for roles involved in the development and maintenance of websites and web applications. Web developers are responsible for either front-end or back-end development.

POLICY

A. Applicability

This policy, and its accompanying Web Application Security Standard, apply to all University Community Members and other users of University Information wherever located, including all third-party individuals or entities granted access to University Information. Additionally, this policy establishes and outlines requirements that apply to University Web Applications (including those that are designed for use on mobile devices) that:

- Are hosted on University-managed networks or hardware;
- Are institute and other sites operated under the auspices of NAU employees or third-party vendors or providers;
- Function at the "nau.edu" top level domain ("TLD"); or
- Use or incorporate the University's trademarks, service marks, logos, or other indicia.

B. Information Security Program

In collaboration with the Director of Information Security Services and the Information Security Committee, the CIO, or their designee, oversees and directs a comprehensive Information Security Program to protect and preserve the availability, confidentiality, and integrity of University Information. The program supports the University's compliance with all applicable statutory, regulatory, policy, and contractual guidance or requirements, and is shaped by industry best practices. This policy and its accompanying Web Application Security Standard are an integral part of this comprehensive Information Security effort. All University units and personnel who administer, maintain, create, or develop Web Applications are responsible for implementing the appropriate Web Application classification and security procedures as outlined in this policy and the Web Application Security Standard described below, where applicable under the University's management.

C. Additional Roles and Responsibilities

1. The Director of Information Security Services shall serve as the University's primary enforcement officer for purposes of this policy.

2. At the direction of the Chief Information Officer, or their designee, and its director, Information Security Services provides services such as network monitoring, Web Application assessments and scanning, threat modeling assistance, incident response, and guidance for complying with Information Security controls.

~~3. System administrators shall coordinate with Information Security Services to perform security testing and scanning and collaborate with Web Application developers to apply Web Application protections in accordance with criticality ratings as appropriate.~~

~~4.~~ Development teams responsible for developing University managed Web Applications will perform static code analysis during active development cycles. ~~Web developers shall coordinate with Information Security Services to perform security testing and scanning and collaborate with business units to establish an inventory and criticality ratings for Web Applications as appropriate.~~

D. Web Application Security Standard

The CIO, or their designee, in collaboration with the Director of Information Security Services, establishes and revises, as necessary or appropriate, a comprehensive Web Application Security Standard. All University units and personnel that develop or administer Web Applications designed to manage, or that depend on, University Information must meet the minimum applicable requirements established therein. Individual units may, in collaboration with Information Security Services, adopt additional standards that exceed these minimum requirements. The CIO, or their designee, may grant a written exemption to Web Application security requirements when the CIO, or their designee, determines that doing so is in the best interests of the University.

E. Duty to Report

All University Community Members are obligated to immediately report any IT security threat or suspected or actual release or breach of Sensitive Data or Highly Sensitive Data, as these terms are defined in the University's Data Classification and Handling policy. **Dial 928-523-3335 to make a report**. In collaboration with appropriate University stakeholders, Information Security Services is responsible for notifying all affected and responsible parties. In the event of a security incident ~~T~~the CIO, or their designee, ~~will~~ may assemble an incident response team to investigate, preserve evidence, mitigate the situation, ~~and~~ analyze, and report. ~~on the event~~nt. If health or safety may be a concern, the reporting party or Information Security Services shall immediately notify the Northern Arizona University Police Department and any other external entity or governmental agency as appropriate.

F. Compliance and Enforcement

As outlined in the University's Information Security policy, when necessary to protect the integrity or security of its IT Resources or information systems and the University Information they contain, the University may suspend access to its networks or devices and may examine any user account. At the discretion of the CIO, or their designee, enforcement of this and related IT policies may include the removal of devices or systems from the University's information networks until compliance with applicable requirements is achieved. Violations by a University Community Member of the duty and responsibility to protect the University's data, IT Resources, and information systems in accordance with this and other applicable policies, standards, or requirements may also result in denial of access to University Information and/or University IT Resources or the temporary or permanent revocation of access privileges. Individuals who violate this policy are subject to disciplinary action under applicable Arizona Board of Regents and University conduct policies up to and including expulsion or termination and possible civil liability or criminal prosecution. In cases where full compliance with the requirements of this policy may not be immediately achievable, the unit's leadership must consult with Information Security Services to develop a plan for mitigating risk while working to achieve compliance as soon as possible.

RESPONSIBILITIES

Chief Information Officer: update and publish, as necessary and appropriate, the University's *Web Application Security Policy* and its accompanying Web Application Security Standard; appoint and direct a Director of Information Security Services.

Information Security Services: conduct security scans and provide guidance, advice, and recommendations to business units and web developers for mitigating web application security vulnerabilities and risks.

Director of Information Security Services: reporting to the CIO, or their designee, ~~,~~ is responsible for working with the roles identified herein to develop and implement security policies, procedures, protocols, and standards in support of this policy and the Information Security Program; implement and serve as the primary enforcement officer for this policy.

System Administrators: follow best practices in the secure implementation and maintenance of servers, web application firewalls, and University IT Resources.

University Community Members: implement the requirements of this policy within their respective areas of responsibility; adhere to the *Appropriate Use of Information Technology Resources* policy. Business units that own a Web Application have the additional responsibility to work with web developers to establish a Web Application inventory and availability and criticality ratings, as appropriate, in accordance with this policy.

Web Developers: follow current best practices and receive periodic training in the secure development of Web Applications.

PROCEDURES

Various procedures associated with this policy are outlined in the *Web Application Security Standard* document.

RELATED INFORMATION

Forms or Tools

Web Application Security Standard

Cross-References

Appropriate Use of Information Technology

Auditing, Logging, and Monitoring

Data Classification and Data Handling

Enterprise System Change Management

Information Security Policy

Information Technology Incident Management

Sources

Arizona Board of Regents Policy

- 9-201
- 9-202

APPENDIX*

Web Application Security Controls and Threat Modeling

*Disclaimer: all documents, links, or other materials included in this policy's appendix are provided solely for the user's convenience and are not part of official University policy.