



UNIVERSITY POLICY IT-07.00-08/22

TO: The University of West Florida Community

FROM: Dr. Martha D. Saunders, President

SUBJECT: UWF Server Administration

RESPONSIBLE OFFICE: Information Technology Services

I. Purpose:

This policy establishes standards for the administration and configuration of computer servers to maximize safety and security while minimizing support costs to the University.

II. Definitions:

Chief Information Security Officer (“CISO”) – The UWF employee who serves as the first point of contact for all security-related queries from UWF administration.

Confluence – A Wiki that is configured to allow authenticated access and provides special templates and integrated features that enhance UWF’s ability to document and publish business processes.

Local Support Provider (“LSP”) – A UWF employee with an Information Technology skillset who has duties and responsibilities to provide technical support to a subset of the UWF organization (Department or Division). LSPs are considered by the Department of Information Technology Services to be professionals in their field and are provided technical and software tools, expanded access to certain systems, and occasional training.

Server – UWF-owned computer (virtual or physical) or UWF-managed computer that is part of a network and provides electronic services to other computers, directly to the public, or to UWF-affiliated persons.

Wiki – Software that allows self-publishing.

III. Policy:

A. Configuration

All Servers deployed on the UWF network or utilized by UWF will be configured to a minimum standard (“Server Configuration Standard”) designed to safeguard the

University's protected information and data on the UWF network and on public networks. The Server Configuration Standard is located in the LSP "space" in Confluence. The access to this page is restricted to LSPs.

B. Exemptions

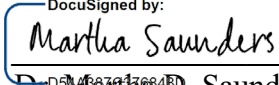
Submissions for exemptions from this Policy must be submitted by the LSP for the department or unit and will be reviewed by the UWF CISO or designee. Approval will be based on the Server's explicit business purpose or approved technical limitations. Appropriate compensating controls may be required for the Server's use. To request an exemption for a Server, an ITS Request Jira ticket should be submitted through the University's service desk system.

C. Accountability

The Internal Audit Department, with advice and assistance from the Information Technology Services Department, will periodically monitor for compliance with this policy and the controls created to safeguard UWF and its assets.

D. Compliance

Violations of this policy may lead to the suspension or revocation of system privileges and disciplinary action up to and including termination of employment. UWF may report to appropriate authorities any violation of the law.

Approved by:  **Date:** 09/12/2022
Dr. Martha D. Saunders

Authority: Florida BOG Reg. 1.001, University Board of Trustees Powers and Duties
Florida BOG Reg. 3.0075, Security of Data Related Information Technology
Resources

History: Created 09/12/2022