**Who Should Know This**
These guidelines apply to IT workers who manage web servers, web application developers and web content managers. Web server managers should read and understand this information before accessing, storing, or transmitting Restricted Data [2].

**Definitions**
- **Web Server**: A computer service to client software running on other computers usually using the hypertext transfer protocol (http). More specifically, a web server is a computer that manages and shares web based applications and data accessible anytime from any computer connected to the network (Internet or Intranet).
- **Web Server Manager**: The individual or group that manages the web service and usually the computer system on which it runs.
- **Web Application Developers**: The individual or group that creates computer applications that will be made available via a web server.
- **Web Content Managers**: The individual or group that creates and maintains information available via a web server.

**Purpose**
The purpose of this document is to establish and promote secure web server management guidelines to avoid unauthorized disclosure of Restricted Data. This document is also intended to facilitate compliance by providing one document that combines references to other relevant standards and guidelines.

**Guidelines**
Listed below are safeguards to protect Restricted Data accessed, stored, or transmitted on UF Web servers.

1. Web server managers, web application developers and web content managers should maintain awareness of the risks and responsibilities of supporting a web-based computing environment.
2. Web servers should be managed by UF professional IT workers or a support service approved by the Level 2 Unit ISM. The web server manager must comply with the UF IT Security Regulations and configure servers accordingly. Practices to maintain confidentiality, integrity, availability, and currency of web content must be consistent with Data Principal requirements.
3. Where possible, Restricted Data should not be stored directly on a web server. If Restricted Data needs to be stored directly on a Web server:
   a. It should be the minimum amount of data to accomplish the task.
   b. Access to that data should confer the least privilege to accomplish the task.
   c. Encryption of the data storage should be considered based on risk determined by the Data Principal or Level 2 Unit ISM. The type of encryption and the key length should also be determined by the Data Principal and Level 2 Unit ISM in coordination with the Data Custodians.
d. For web servers that contain Restricted Data, backups should be consistent with the UF Guidelines for IT Workers to Protect Restricted Data on Backup Media [9].

4. Regardless of where the data is stored, web servers that provide access to Restricted Data should also provide facilities to secure transmission of the data such as SSL certificates, signed by a trusted authority. If data will be accessible from public networks or any wireless network, including UF wireless networks, facilities to encrypt transmission must be provided. The transmitted data should be the minimum amount necessary to accomplish the task.

5. Facilities must be provided to authenticate and authorize access to Restricted Data accessed from a web environment, regardless of where the data is stored.

6. A process to routinely audit for unauthorized disclosure of Restricted Data via the web server should be documented and implemented. Example monitoring processes include web search engines, manual system search, or commercial and open-source search tools such as Watchfire [7] (not an endorsement) or Cornell’s Spider [8] (not an endorsement). See the UF IT security web site for information about other data discovery tools [11]. Procedures must be consistent with the UF Incident Response Policy and the UF Privacy Policy. The following should be included:
   a. Immediate removal of unauthorized access to the data.
   b. Procedures to protect meta information of exposed files containing Restricted Data for forensic analysis.
   c. Immediate notification of UF Privacy Office, Data Principal, and Level 2 Unit ISM.

7. Web application development should follow the UF Guidelines to Develop Application for Secure Deployment [10].

8. Hosts that store and serve web content must be maintained according to the Network and Host Security Standard [3].

9. End-user functions and web-server functions should not be performed on the same computer (i.e., email, web surfing and other end-user functions should not be performed on a computer that provides web service, and web service should not be provided from an end-user workstation computer).

10. Access to modify the data and applications served by the web server should be restricted to the least privilege for their purpose and be consistent with Data Principal requirements. A Content Management System (CMS) may provide an alternative method of maintaining Web site content while minimizing access to restricted directories.

11. Access to the server storage areas for log, configuration, and binary files should be restricted to the least privilege for their purpose and be consistent with Data Principal requirements. Access to these areas should be restricted to a very few people who perform operational support of the web server.

12. The web service should run with minimum privileges necessary to perform its function. Example methods include a virtual machine, a sandbox, or a jailed environment.

13. Accounts with access to the host running the web service and accounts with access to hosts that store data for the web service should have the minimum privileges necessary for their function.

14. Access to web content should be reviewed for compliance with confidentiality requirements during development and upon publication.

**Bibliography**

UF Guidelines for IT Workers Who Support Web-Based Services Used with Restricted Data