1. **Background**

The University of Cincinnati (UC) data network is a shared resource used by the entire university community and its affiliates in support of the university's business practices and academic missions. Access to the data network is both an essential tool for university life and work and a valuable privilege. University units and community members must cooperate to protect the network by securing computer, server and network devices in order to preserve that access.

The UCIT Office of Information Security (OIS) is responsible for the efficient, effective and secure operation of the university data network. Concurrently, academic, administrative and support units (referred to as “units” from here on) are responsible for the efficient, effective and secure operation of their local networks.

The Web Server Security Standard (WSSS) establishes security requirements for web servers, web applications, and web services that are critical to UC. The standard is intended to help protect the university’s central and distributed telecommunications and computing environment from accidental or intentional damage. The standard is intended to protect the university’s connected assets from alteration or theft of data while preserving university community members’ appropriate access and use.

The WSSS is one of the interrelated Security Standards, each of which addresses a different aspect of computer, network and data security.

This is a security standard for critical web servers. Other standards and policies may set the security standards for non-server computers (laptops, desktops, etc.).

In addition to the WSSS and interrelated Security Standards, users must comply with UC’s Data Protection Policy, Vulnerable Electronic Systems Policy, and Use of Information Technology Policy.

This standard applies to database servers that have been deemed “critical” based on the criteria listed in the third section of the Critical Server Security Standard (CSSS), whether owned or managed by the university, a university community member or a 3rd party organization, and that connects to the university data network or support infrastructure either directly or indirectly.

This standard outlines the responsibility of all university community members, including students, faculty, staff, agents, guests, or employees of affiliated entities. This includes (a) individuals who connect a device, either directly or indirectly, to the university data network or support infrastructure, (b) individuals who install, maintain, or support a critical server, (c) individuals who develop, deploy, or maintain an application that resides or runs on a critical server, and (d) individuals who maintain or support a web server, or anyone who develops, deploys, or maintains a web application or other web content.
2. **Implementation Guidance**

Since the scope of the DSSS encompasses an audience that does not necessarily include those well versed in information technology and might include other general users, the following section is meant to outline not just the intent but also some platform specific guidance to aid in meeting the requirement of the standard. This implementation guidance can be found in supporting documents on this site or by contacting OIS at infosec@uc.edu.


3.1. The server hosting the web server, web service, or web application must comply with the Client Computing Security Standard (CCSS) and Critical Server Security Standard (CSSS).

All servers that host web servers, web services, or web applications and that have been deemed 'critical' based on the criteria in CSSS must comply with this standard.

This standard applies to all servers that have been deemed “critical” based on the following criteria:

3.1.1. It contains or serves Restricted Data, as defined in the Data Protection Policy.
3.1.2. Loss of service carries a significant financial liability, including grants and/or contracts.
3.1.3. Loss of service results in a significant negative impact(s) for the unit or for the reputation of the university.
3.1.4. Unit, OIS or university administration deems the server to be critical.

Requests to connect servers to the UC network that are not owned by the university must be reviewed and approved by OIS via a Risk Acceptance Form prior to placing the server on the network. When equipment that is not owned by the university is placed on the network, the equipment owner consents to vulnerability scans of the equipment by OIS, departmental staff or both.

3.2. **Installation and Configuration**

Since often web servers exist as applications on a host operating system, they require special considerations during the configuration and installation phase of deployment.

3.2.1. Technical Staff MUST:

- **3.2.1.1.** Configure web services in accordance with vendor security recommendations.
- **3.2.1.2.** Ensure that only those web services or applications specifically needed should be enabled. Web services, applications, and sample content which is not needed should be disabled.
- **3.2.1.3.** Patch web server software and web applications to all current security patches, as required by the CSSS. Software developed by vendors or developers unresponsive to patching security vulnerabilities should be replaced with alternative software. If alternative software is not available, a responsible party may assume patching responsibility, or compensating controls must be put into place.
- **3.2.1.4.** Configure the web server to allow access only to data that is meant to be publicly available. Configure a robots.txt file to properly protect content from automatic collection by web crawlers. "Obscure" or "secret" file or directory names must NOT be used to protect content.
- **3.2.1.5.** Monitor comments on blogs and other forums if anonymous posting is allowed. This responsibility may be delegated to non-technical staff as deemed appropriate by the department or unit.
3.2.1.6. Prohibit web servers and web applications to run with elevated privileges (e.g. “root” or “Administrator”).
3.2.1.7. Use secure mechanisms to allow developers to install new or update existing content. Traditional FTP or other unencrypted password-based systems must not be used. Alternative protocols that provide encryption and secure authentication (e.g. SSH/SCP, SFTP, and rsync/SSH) must be used.

3.2.2. Technical Staff SHOULD:

3.2.2.1. Store content uploaded through web applications outside of the document root.
3.2.2.2. Limit the ability of web server and web application user accounts to modify other programs, logs, or system configuration files by limiting account privileges.

3.3. Logging

3.3.1. Technical Staff MUST:

3.3.1.1. Develop or configure web servers and applications to write logs that are adequate for incident response and security investigations. Useful log information includes, but is not limited to: Failed and successful login attempts, Account privilege changes and Timestamp information. Logs must contain the URLs as requested by the client. Logs must be retained for a minimum of 90 days in a safe and secure manner, limiting all user write access to ensure log integrity, as per the CSSS.
3.3.1.2. Keep discrete log files for each virtual web server if there are multiple virtual web servers hosted on a single server instance.
3.3.1.3. Copy web service logs to a separate secure log server for retention.
3.3.1.4. Ensure that all system times are standardized and that logs reflect those standardized time settings.

3.4. Encryption

3.4.1. Technical staff MUST:

3.4.1.1. Encrypt all Restricted Data (as defined by the Data Protection Policy).
3.4.1.2. Use commercially signed or authorized certificates for web services outside of the department or unit.
3.4.1.3. Renew certificates before their expiration date.

3.5. Secure Software Design, Implementation, and Testing Procedures

3.5.1. Unit Administrative Staff SHOULD:

3.5.1.1. Train those who develop web applications in secure code design, implementation, and testing procedures.
3.5.1.2. Review code to identify and correct common mistakes where possible or appropriate before deployment.

3.5.2. Technical Staff SHOULD:

3.5.2.1. Prevent the error messages from underlying systems and processes from being publicly available to the web browser.
3.5.2.2. Only use active client-side and server-side content when absolutely necessary, and then with extreme caution.
3.5.2.3. Frequently and regularly scan web services for vulnerabilities (e.g. SQL injection flaws, cross-site scripting).

3. Compliance

4.1. Standards Compliance

All designated critical servers must comply with the CCSS, CSSS and WSSS.

In some cases it may not be possible to bring a server into compliance. For example, older laboratory equipment and/or software may not operate with current operating systems or security patches. In these special cases units must employ compensating controls to meet the requirements of this standard. In rare cases an exception may be made by completing a Risk Acceptance Form if no compensating control is possible.

Units must internally document requested compensating controls and any exceptions. These must be reviewed, tested, and approved by OIS and the unit must retain the approved documentation for audit so long as the server is in operation.

Note: Servers that are not in compliance of this standard and/or do not have an approved Risk Acceptance Form may not be connected to UC's network.

4.2. Registration of Critical Servers

Units are required to register all critical servers with OIS. Technical staff must register all IP addresses and DNS host names and 24/7 contact information for the administrators who are responsible for the servers. Information identifying the controlling unit is also required.

Units are expected to maintain local records of critical servers as well.

4.3. Role of Units, IT staff, and Others

The unit is responsible for ensuring compliance with the WSSS, though IT staff may perform the actual implementation on university owned/managed equipment.

The user is responsible for compliance on personally owned equipment. Users granted responsibility for administration on university owned/managed equipment will share responsibility for compliance with local IT staff. (i.e. local administrator rights, users granted access via a local administrative privilege standard policy.) See the Local Administrative Privilege Standard (LAPS) for additional information.

Users who do not comply with this standard are in violation of the Data Protection Policy, Vulnerable Electronic Systems Policy, and/or Use of Information Technology Policy. In accordance with those policies, violators may be denied access to university computing resources and may be subject to other penalties and disciplinary action including university disciplinary procedures.

Units are required to register all critical servers with OIS. Technical staff must register all IP addresses and DNS host names and 24/7 contact information for the administrators who are responsible for the servers. Information identifying the controlling unit is also required.

Units are expected to maintain local records of critical servers as well.
4.4. Role of the UCIT Office of Information Security

OIS is tasked with the responsibility of maintaining the WSSS standard and ensuring that the documentation is kept current with threats and technologies going forward. OIS will include community feedback and do publicity for any changes to the document.

OIS will review and approve or deny Risk Acceptance Forms.

OIS staff members are identified as the enterprise subject matter experts on information security practice and policy and in that role can be asked to perform security assessments or consultations with units.

4.5. Compliance Mechanisms

Compliance with the standard can be accomplished using a variety of technological or practical tools. Units that have the capability to perform automated detection of patches and vulnerabilities should use these tools to do regular inspection of their networks to gather information regarding the state of compliance.

Those units that do not have the capability to run automated tools to gather compliance information are encouraged to consider purchasing/acquiring these tools but may elect to use a manual process such as spot inspection of servers to determine overall compliance.

NOTE: Units must conduct a compliance inventory on all university-managed devices no less than a quarterly basis.

OIS may conduct an inspection of unit resources in cooperation with the unit leadership and IT staff to determine overall CSSS compliance. These spot inspections are required if a unit is confirmed through investigation to have been involved in a CSSS related data breach.

Devices found not to be in compliance must be quarantined from the general network and the compliance issue must be addressed before it may be restored to normal operation. If the device cannot be made compliant the unit may implement a compensating control or request an exception. Upon approval of the exception request the device may be restored to normal operation.

5. Review

OIS must review this document and must update or modify the standard requirements as necessary on at least an annual cycle.

6. Definitions

Automated – when an update or patch is made available, it is automatically downloaded and applied without requiring manual intervention. Availability can be determined by the administrator of the system after a testing period or upon release from a vendor. The discretion is in the hands of the unit to determine how to apply patches and test them to prevent conflicts with software but it is expected that this process be done in a prompt and timely manner so as to keep systems current with security releases and protect against exploits and vulnerabilities.

Audit – a log or other function on a device that provides an evaluation of a system, process, enterprise, project, or product.

Authentication – access to the device provided by controls such as account identifiers (user names) and robust passwords.
**Compensating controls** – a method of addressing the risk associated with a standard requirement by using alternative techniques to mitigate the risk. Compensating controls are documented on the Risk Acceptance Form.

**Computer** - a desktop, laptop or mobile device (including tablets, smart phones, PDA’s, etc.) that is used primarily for normal desktop application work. With regards to the WSSS, computer does not include computing devices with a dedicated use like building control systems or dedicated appliances that perform only a dedicated function. *This definition does not exclude desktop systems traditionally used for desktop purposes that are re-tasked for use in non-traditional roles (i.e. lab instrument control).*

**Contains or serves Restricted Data** - servers that contain or serve Restricted Data and servers that have significant risk of exposing Restricted Data. Obvious cases include web, file, mail and database servers that either contain Restricted Data or which provide access to Restricted Data. These present a higher risk to the University since exploitation of vulnerabilities in the network services that they provide could lead to exposure of Restricted Data. There are non-obvious cases as well. For example, *web servers that have applications which access database servers that contain Restricted Data are also high risk, since the Restricted Data could inadvertently be exposed through attacks against the web applications (such as SQL injection attacks), even though the web server doesn't intentionally provide access to Restricted Data and doesn't itself contain Restricted Data.*

**Current** – Timely, Up-to-date, and Reasonable. The definitions for these terms throughout the standard have been left purposefully elastic to allow for situations and use cases throughout the university. In the case of "Reasonable" and "Timely", units are urged to help define these terms in their policy and procedures. Adding a specific time frame may not be appropriate to all situations. "Current" and "Up-to-date" are also flexibly defined as not every device or security technique can be implemented, tested and vetted immediately and units need time to consider the impact of changes on the programs, hardware and end users. OIS does not want to encourage or force reckless changes on the university environment in the name of security. OIS strives to merely promote proper implementation in the proper time frame. If you have questions about local policy and if units are concerned that these terms are being applied too flexibly and process or procedures are not properly addressing security concerns OIS will be happy to review and suggest options upon request.

**Data Custodian** – a university unit or employee responsible for the operation and management of systems and servers which collect, manage, and provide access to institutional data.

**Data network** – a group of interconnected computers managed by the University of Cincinnati.

**Data Steward** – a university official with direct operational responsibility for one or more types of institutional data

**Data Trustee** – a senior university executive with management and policy responsibility for areas of institutional data

**Data User** – a university unit or community member using institutional data in the conduct of university business

**Device** – for the purposes of this standard, device is an interchangeable term with the above definition of “Computer”. Includes any network connectable device, including items such as any fixed or portable computer, laptop or handheld computer, tablet computer, electronic data storage mechanism or removable media, input or output device attached to or used by a computer, personal digital assistant, cellular phone, smart phone, server, printer, copier, scanner, router and other electronic devices that may connect to UC’s network. Devices that are supplied an IP address from UC’s network are also included. This definition is flexible but units should use best judgment in interpreting what computing devices are of concern with the WSSS. While the above definition could be interpreted as including
devices like keyboards and mice, devices of this nature are not considered relevant unless they are subject to attacks or exploits - for instance because of inbuilt storage or an operating system.

**Exemption** – an approved exception to a standard. See the definition below for “Risk Acceptance Form”.

**Firewall software** – a part of a data network that is designed to block unauthorized access while permitting authorized communication. Firewalls can be software or dedicated computers that are configured to control computer traffic between different computer networks based upon a set of rules and other criteria. Devices that do not have a native firewall capability can be protected by a firewall appliance from external attacks but if a device or the operating system of a device has a firewall intrinsic to it (i.e. Windows and Mac built in Firewalls) or the capability to run a local software firewall (like Zone Alarm, etc.) then that firewall must be enabled to satisfy the WSSS requirement.

**Logging** – the process of recording events from a system, process, enterprise, project, or product such as attempts to successfully or unsuccessfully authenticate to a system.

**Manually** – updated through a manual process, this process can include some automated tools but is generally accomplished using manpower resources and monitored directly by employees.

**Must** – means that this control must be implemented unless an exception has been specifically requested and granted (typically with some sort of compensating control).

**Must ... if technically possible** - means that this control must be implemented if the product supports it. Locally developed software must be modified to provide necessary features in these cases. Performance issues can be considered in determining whether something is “technically possible”, although it is better if systems can be engineered to provide adequate performance with the security controls in place.

**Non-compliant** – a device that does not meet the requirements of the standard.

**Operating system** - the most important program that runs on a computer. Every general-purpose computer must have an operating system to run other programs/software.

**Password** - a sequence of characters that one must input to gain access to a file, application, or computer system. A password is typically used in coordination with a user name.

**Quarantine** – to isolate the device from other connected devices in a way that protects the device from exposure and prevents the device from potentially affecting the other resources on the data network.

**Reasonable** – see the definition above for “Current”

**Remote Access** - access, usually administrative access, from outside administrative control – i.e. not the console or other directly connected device.

**Restricted Data** - specific data or data types defined in the [Data Protection Policy](#) are restricted in nature.

**Risk Acceptance Form** – in rare cases an exemption may be made if a device cannot be brought into compliance with one or more of the WSSS elements and the element(s) cannot be addressed via a compensating control or controls. The [Risk Acceptance Form](#) must be submitted to OIS who will review and approve or deny the requests.

**Security Incident** - computer security incidents occur when a security policy or standard has been violated. Examples include theft; virus, spyware and other malware infections; unauthorized logons;
unauthorized access to Restricted Data; unauthorized changes to the system and other similar situations.

**Should** - means that this control is a good security practice, but is not required for compliance with this standard. An exception does not need to be requested/granted in cases where you do not implement "Should" items.

**Supported** – software and hardware that is currently receiving security updates by the manufacturer.

**Timely** – see the definition above for “Current”

**UC Network** – the University of Cincinnati data network.

**Unit** – for the purposes of this standard, unit is used to describe an academic or administrative entity of the university. This organization may include an office, department, division, or college depending on the organizational structure defined by the university.

**University-managed devices** – devices purchased, owned, gifted, granted and/or maintained by university employees. University-owned devices can include supported computer systems and devices purchased through any of the various funding models including but not limited to grants, endowment, direct purchase, etc.

**Unsupported** – software that is no longer supported, may qualify for an exemption under the compensating control and exemption process. See “Exemption” and “Risk Acceptance Form” for more information.

**Up-to-date** – see the definition above for “Current”

**User name** – a specific log in identity assigned to an individual user. User names are typically used to gain access to a computer operating system or application. Generic user names are generally prohibited, but may be permitted in certain circumstances with an approved Risk Acceptance Form.

**Viruses, spyware or adware** – a group of computer programs classified as “bad” or malware. Viruses, spyware and adware often exploit flaws in computer programs and operating systems to extract information or attack the integrity or availability of a data network. These programs are usually malicious or undesired software.

**Web browser** - a computer program used for accessing sites or information on a network (such as the World Wide Web).

7. **Tools**


8. **Related links**

   [Security Standards]
   [Data Protection Policy]
   [Vulnerable Electronic Systems Policy]
   [Use of Information Technology Policy]

9. **Phone Contacts**
Appendix A

Web Server Security Standard
Evaluation Checklist for Critical Web Servers

A web server is “critical” if it meets at least one of the following criteria:

1. It contains or serves Restricted Data, as defined in the Data Protection Policy.
2. Loss of service carries a significant financial liability, including grants and/or contracts.
3. Loss of service results in a significant negative impact(s) for the unit or for the reputation of the university.
4. Unit, OIS or university administration deems the server to be critical.

<table>
<thead>
<tr>
<th>Statement</th>
<th>Must or Should?</th>
<th>Met</th>
<th>Not Met</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before using a computer on UC’s network, users must comply with UC’s Data Protection Policy, the Vulnerable Electronic Systems Policy and the Use of Information Technology Policy.</td>
<td>Must</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Complies with Client Computing Security Standard (CCSS).</td>
<td>Must</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Complies with Critical Server Security Standard (CSSS).</td>
<td>Must</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Complies with Database Server Security Standard (DSSS).</td>
<td>Must</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Complies with Web Server Security Standard (WSSS).</td>
<td>Must</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Installation & Configuration**

- Configure web services according to vendor security recommendations.
- Configure server to use ONLY needed web services or applications.
- Install all required updates and security patches prior to deployment of web server.
- Configure server to only display public data.
- Configure "robots.txt" or similar files to protect content.
- Configure Moderation or assign personnel to monitor any blog or forum content if anonymous posting is allowed.
- Prevent web servers or web applications from executing with “elevated” or admin privileges.
- Use secure mechanisms to allow developers to install new or update existing content. Do not use traditional FTP or other unencrypted password-based systems.
- Store all uploaded web content outside of document root.
- Configure web services and web applications to use limited named accounts when modifying other programs, logs or configuration files.

**Logging**

- Configure web servers or applications to write logs containing login attempts (successful or failed), account modification (privilege changes, promotion, creation, deletion), timestamp, client access URLs.
- Configure log retention of 90 days in a safe and secure manner, limiting all user write access to ensure log integrity and plan for adequate storage space.
- Create discrete logs for each server instance.
- Copy web server/application logs to another log management server or location.
- Ensure that all system times are standardized and that logs reflect those standardized time settings.

**Encryption**
<table>
<thead>
<tr>
<th>Action</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure web server/application to use SSL/TLS encryption to transfer/display restricted data.</td>
<td>Must</td>
</tr>
<tr>
<td>Obtain a signed or authorized commercial certificate for web services accessed outside of the department/unit.</td>
<td>Must</td>
</tr>
<tr>
<td>Renew certificates prior to expiration</td>
<td>Must</td>
</tr>
<tr>
<td><strong>Secure Software Design, Implementation, and Testing</strong></td>
<td></td>
</tr>
<tr>
<td>Ensure all web developers follow secure code design, implementation, and testing procedures.</td>
<td>Should</td>
</tr>
<tr>
<td>Review code prior to updates/integration for coding errors and common mistakes.</td>
<td>Should</td>
</tr>
<tr>
<td>Prevent error messages from publicly displaying information about underlying systems/processes or software.</td>
<td>Should</td>
</tr>
<tr>
<td>Only use active client-side and server-side content when absolutely necessary, and then with extreme caution.</td>
<td>Should</td>
</tr>
<tr>
<td>Scan web services for vulnerabilities.</td>
<td>Should</td>
</tr>
<tr>
<td>Scan web applications for vulnerabilities</td>
<td>Must</td>
</tr>
</tbody>
</table>