Database Server Security Standard (DSSS)

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 IT@UC 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 Database Server Security Standard (DSSS) establishes security requirements for database servers 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 DSSS 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 database servers. Other standards and policies may set the security standards for non-server computers (laptops, desktops, etc.).

In addition to the DSSS and interrelated Security Standards, users must comply with UC’s Data Governance & Classification Policy, Vulnerable Electronic Systems Policy, and Acceptable Use of University Information Technology Resources.

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, and (c) individuals who develop, deploy, or maintain an application that resides or runs on a critical server.

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. The Database Server Security Standard (DSSS)

3.1. The server hosting the database must comply with the Client Computing Security Standard (CCSS) and Critical Server Security Standard (CSSS).

All servers that host databases, database services, or database applications and that have been deemed “critical” based on the criteria in the Critical Server Security Standard (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 Governance & Classification 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. Network and Firewalls

Special considerations are required when configuring network and host based firewalls to protect database servers, which go beyond the requirements specified in the Critical
Server Security Standard (CSSS). These are:

3.2.1. Technical Staff MUST:

3.2.1.1. Configure network and host-based firewall rules to restrict access to the database server as much as possible. In particular, access should be restricted to UC address space, or if applicable only to those servers which access the database. Off campus access should be done through a VPN or similar encrypted remote access strategy.

3.2.1.2. Ensure that database connectivity APIs such as ODBC or JDBC do not store their connection information (especially account names and passwords) unencrypted, if technically possible. Where technically possible, disable or configure tracing functions so that they do not capture authentication information in their logs.

3.2.2. Technical Staff SHOULD:

3.2.2.1. Encrypt the network session or use an encrypted or one-time authentication system to protect the database server from sniffing and replay attacks.

3.3. Installation and Configuration
Since often database servers exist as applications on a host operating system, those that meet the requirements of this standard also require special considerations during the configuration and installation phase of deployment.

3.3.1. Technical Staff MUST:

3.3.1.1. Ensure that database servers are not hosted on the same server as the associated web server with their associated web servers.

3.3.1.2. Install and configure database software in accordance with vendor security recommendations.

3.3.1.3. Ensure that only database administrators and system administrators will have operating system login access on the database server.

3.3.1.4. Run database servers under accounts without administrative or root privileges whenever technically possible.

3.3.1.5. Use a version of database software that is currently supported by the vendor or open source project, as required by the Critical Server Security Standard.

3.3.1.6. Disable and remove unused software components and all unnecessary features, if technically possible.

3.3.2. Technical Staff SHOULD:

3.3.2.1. Run only database server application scripts supported and controlled by the database or system administrators.
3.4. Accounts, Passwords and Privileges

Database servers that fall under this standard require special consideration when identifying access configuration. Database servers that contain Restricted Data are required to meet the following account access, password and privilege configurations:

3.4.1. Technical Staff MUST:

3.4.1.1. Provide database and system administrators with their own OS accounts. No group accounts are permitted.
3.4.1.2. Login to the server using their own accounts rather than logging in as root or Administrator.
3.4.1.3. Create separate accounts for running automated tasks (backups, replication, etc.) that do not allow direct logins. Administrators must not use these accounts for other tasks.
3.4.1.4. Ensure that the OS account that the database server runs under does not allow direct logins.
3.4.1.5. Provide individuals who need direct database access with their own accounts. Applications that do their own authentication do not need to use separate database accounts for each user.
3.4.1.6. Provide each application (including web applications and automated processes) with its own database account.
3.4.1.7. Use the principle of least privilege when assigning access rights to operating system and database accounts. This is especially important for application accounts - these must only have access to the parts of the database that are needed.
3.4.1.8. Use strong passwords for all accounts as defined in the Password Policy.
3.4.1.9. Configure database accounts to lock for 15 minutes after 5 failed connection attempts, if technically possible.
3.4.1.10. Audit accounts and associated privileges monthly and remove or disable accounts and privileges when they are no longer needed.

3.4.2. Technical Staff SHOULD:

3.4.2.1. Manage database permissions through roles or groups rather than for each separate account.

3.5. Restricted Data

Sometimes Restricted Data must be stored in database servers for use in search or other functions. All database servers under this standard must take appropriate steps to safeguard any Restricted Data maintained within them and meet the following requirements:

3.5.1. Technical Staff MUST:

3.5.1.1. Ensure that the procedures set forth in the Data Governance &
Classification Policy are followed if Restricted Data are stored in the database.

3.5.1.2. Prevent the use of "real" Restricted Data in testing or development environments. If this cannot be done, then ensure that the testing or development environments conform to the Critical Server Security Standard and this standard.

3.5.1.3. Use a redacted version of Restricted Data if technically possible.

3.5.1.4. Use encryption to protect Restricted Data if technically possible.

3.5.2. Technical Staff SHOULD:

3.5.2.1. Hash Restricted Data if it is only used for searches.

3.6. Auditing and Monitoring

Database servers that meet the requirements of this standard or contain Restricted Data and as a result administrators are responsible for knowing what data is located on their servers. Administrators must implement and utilize practices that allow for the audit and monitoring of database systems containing this data by:

3.6.1. Technical Staff MUST:

3.6.1.1. Log the creation, alteration or deletion of database accounts, storage structures, objects and tables.

3.6.1.2. Log enabling and disabling of and any changes to audit functionality.

3.6.1.3. Log granting and revoking of access rights.

3.6.1.4. Log all connection failures. Where technically possible, audit all successful and unsuccessful connection attempts.

4. Compliance

4.1. Standards Compliance

All designated critical servers must comply with the Client Computing Security Standard, Critical Server Security Standard and DSSS.

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.

4.1. 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.

4.2. Role of the IT@UC Office of Information Security

OIS is tasked with the responsibility of maintaining the DSSS 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.

4.3. 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 on 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 DSSS compliance. These spot inspections are required if a unit is confirmed through investigation to have been involved in a DSSS 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 DSSS, 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 DSSS. 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 DSSS 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 Governance & Classification 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 DSSS 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**

   Appendix A - Database Server Security Standard (DSSS) Evaluation Checklist

8. **Related links**

   Security Standards

   Data Governance & Classification Policy

   Vulnerable Electronic Systems Policy

   Acceptable Use of University Information Technology Resources

9. **Contact Information**

   IT@UC Office of Information Security 513-558-ISEC (4732) Email: infosec@uc.edu
B Appendix A

Database Server Security Standard Evaluation Checklist for Critical Databases

A database 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 Governance & Classification 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 Governance &amp; Classification 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>
</tbody>
</table>

**Network and Firewalls**

- Configure network and host-based firewall rules to restrict core DB server access to UC address space only.
- Configure remote access to the DB server through official VPN or encrypted remote access methods only into identified UC IP space
- Ensure database connections (API’s, ODBC, JDBC, etc.) only share encrypted connection information (Passwords, account names, etc.)
- Disable tracing processes that capture credential information into unprotected/unmanaged logs.
- Encrypt sessions or user encrypted/strong authentication (i.e. 2-factor, one time passwords) to protect from sniffer attacks.

**Installation and Configuration**

- Ensure the DB server is not hosted on the same server as the associated web server.
- Follow vendor security recommendation for configuration.
- Limit OS login access on DB server to DBA account and Sysadmins only.
- Run DB software with non-administrative accounts only.
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure DB is currently in support by vendor and does not violate CCSS and CSSS up-to-date requirements.</td>
<td>Must</td>
</tr>
<tr>
<td>Disable or remove all unused DB features or software.</td>
<td>Must</td>
</tr>
<tr>
<td>Run only DB scripts supported and controlled by database or system administrators.</td>
<td>Should</td>
</tr>
</tbody>
</table>

### Accounts, Passwords, and Privileges

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use named individual accounts for all database or system admins.</td>
<td>Must</td>
</tr>
<tr>
<td>Require users to use only named accounts. Disable root or administrator as login accounts.</td>
<td>Must</td>
</tr>
<tr>
<td>Create distinct accounts for automated processes that do not allow direct login.</td>
<td>Must</td>
</tr>
<tr>
<td>Remove direct logon access to user account the database runs under.</td>
<td>Must</td>
</tr>
<tr>
<td>Create/require unique individual accounts for all users that require direct DB access.</td>
<td>Must</td>
</tr>
<tr>
<td>Create/require unique accounts to applications requiring DB access. (Including web applications and automated processes).</td>
<td>Must</td>
</tr>
<tr>
<td>Assign only required privileges to OS and database accounts. Ensure applications only have necessary rights within the database to prevent exploits.</td>
<td>Must</td>
</tr>
<tr>
<td>Require all accounts to follow Password Policy.</td>
<td>Must</td>
</tr>
<tr>
<td>Configure database lock after 5 failed connections for 15 minutes.</td>
<td>Must</td>
</tr>
<tr>
<td>Perform monthly audit of account privileges and access.</td>
<td>Must</td>
</tr>
<tr>
<td>Use roles to manage permissions in the database; do not customize user access rights.</td>
<td>Should</td>
</tr>
</tbody>
</table>

### Restricted Data

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that the procedures set forth in the Data Governance &amp; Classification Policy are followed if Restricted Data are stored in the database.</td>
<td>Must</td>
</tr>
<tr>
<td>Ensure no “real” restricted data is used in testing or dev environments.</td>
<td>Must</td>
</tr>
<tr>
<td>Encrypt stored restricted data in database.</td>
<td>Must</td>
</tr>
<tr>
<td>Hash restricted data used if only used in searches</td>
<td>Should</td>
</tr>
</tbody>
</table>
### Auditing and Monitoring

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable logging of database account creation, modification or deletion, new</td>
<td>Enable logging of audit functions and disable access to modify logging or</td>
</tr>
<tr>
<td>objects, tables or storage structures.</td>
<td>audit requirements once they are set.</td>
</tr>
<tr>
<td>Enable logging of access right changes.</td>
<td>Enable logging of access right changes.</td>
</tr>
<tr>
<td>Enable logging of connections to the database including: failed or successful</td>
<td>Enable logging of connections to the database including: failed or successful</td>
</tr>
<tr>
<td>attempts.</td>
<td>attempts.</td>
</tr>
</tbody>
</table>

### Compliance

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>All designated critical devices must comply with the CSSS.</td>
<td>Must</td>
</tr>
</tbody>
</table>

### In cases where it is not possible to bring a device into compliance

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Units or individuals must employ compensating controls.</td>
<td>Must</td>
</tr>
<tr>
<td>Units must document compensating controls and must retain this documentation</td>
<td>Units must request an exemption to one or more elements of the standard if</td>
</tr>
<tr>
<td>for audit so long as the device is in operation.</td>
<td>no compensating control is possible.</td>
</tr>
<tr>
<td>Risk Acceptance Form must be submitted to OIS</td>
<td>Risk Acceptance Form must be submitted to OIS</td>
</tr>
</tbody>
</table>

### Registration of Critical Servers

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Units are required to register all critical servers with OIS. Technical</td>
<td>Units are required to register all critical servers with OIS. Technical</td>
</tr>
<tr>
<td>Staff MUST register all IP addresses and DNS host names and 24/7 contact</td>
<td>Staff MUST register all IP addresses and DNS host names and 24/7 contact</td>
</tr>
<tr>
<td>information for the administrators who are responsible for the servers.</td>
<td>information for the administrators who are responsible for the servers.</td>
</tr>
<tr>
<td>Information identifying the controlling unit is also required.</td>
<td>Information identifying the controlling unit is also required.</td>
</tr>
</tbody>
</table>

### Compliance Mechanisms

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>When tools that perform automated detection of patches and vulnerabilities</td>
<td>When tools that perform automated detection of patches and vulnerabilities</td>
</tr>
<tr>
<td>are available, units should regularly inspect their networks to gather</td>
<td>are not available, units should consider purchasing/acquiring these tools.</td>
</tr>
<tr>
<td>information regarding the state of compliance.</td>
<td>Should</td>
</tr>
<tr>
<td>Should</td>
<td>Should</td>
</tr>
</tbody>
</table>

Database Server Security Standard
When tools that perform automated detection of patches and vulnerabilities are not available, units should use a manual process such as spot inspection of computers to determine overall compliance.

Units must conduct a compliance inventory on all university-owned/managed devices on no less than a quarterly basis per the Vulnerable Electronic Systems Policy.

Devices found not to be in compliance must be quarantined from UC’s network and the compliance issue must be addressed before it may be reconnected to UC’s network. If the device cannot be made compliant, the unit must implement a compensating control or have a Risk Acceptance Form approved. Only upon approval of the Risk Acceptance Form may the device be restored to normal operation on UC’s network.

**History:**
Effective Date: 01/15/2015
Revised Date: 3/21/2017