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 Critical Server Security Standard (CSSS) establishes security requirements for 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 also intended to protect the university’s connected assets from alteration or theft of data while preserving university community members’ appropriate access and use.

   The CSSS 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 servers. Other standards and policies may set the security standards for non-server computers (laptops, desktops, etc.).

   In addition to the CSSS 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 servers that have been deemed “critical” based on the criteria in the third section of this standard - whether owned by the university, a university community member or a 3rd party organization - that connect 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 CSSS 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 the OIS at infosec@uc.edu.

3. The Critical Server Security Standard

3.1. The server must comply with the Client Computing Security Standard (CCSS).

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. Physical Security

The physical security of servers deemed critical is just as important as the information and digital security of the contents of the servers.

3.2.1. Unit Administration MUST:

3.2.1.1. Provide an appropriately secured environment to house critical servers that will prevent unauthorized entry, access or theft.

3.2.2. Unit Administration SHOULD:

3.2.2.1. Consider providing levels of environmental protection and monitoring that are commensurate with the risks and consequences of server failure due to loss of power, overheating, theft and other physical risks.

3.3. Backup and Recovery

Ensuring the safety of data requires that units appropriately plan for disaster recovery and restoration of the data on servers that are deemed critical to the university.

3.3.1. Technical Staff MUST:

3.3.1.1. Follow best practices for backing up critical servers.
3.3.1.2. Encrypt backup media including backup tapes that contain Restricted Data.
3.3.1.3. Securely store encryption keys necessary to decrypt the backups separately from the backup media.
3.3.1.4. Document key management procedures for decrypting backups and assure that they are available to more than one person and approved by the Data Custodian and Data Steward.
3.3.1.5. Test and validate backup procedures work at least one time per year for all critical systems.
3.4. Data Destruction

Proper disposal of server storage media containing critical data must be followed.

3.4.1. Technical Staff MUST:

3.4.1.1. Properly sanitize and/or dispose of media containing Restricted Data when the data is no longer needed according to the Data Protection Policy and Asset Disposition Policy.

3.4.1.2. Follow the Surplus Equipment policies and procedures for proper reuse/recycling/disposal of university equipment.

3.5. Intrusion Detection and Security Tools

3.5.1. Technical Staff MUST:

3.5.1.1. Treat and investigate system changes as server security incidents unless it can be determined conclusively that the changes were authorized.

3.5.2. Technical Staff SHOULD:

3.5.2.1. Implement host-based intrusion detection methods that incorporate baseline comparisons.

3.5.2.2. Install a file integrity monitoring system to monitor system changes.

3.6. Incident Response

3.6.1. Technical Staff MUST:

3.6.1.1. Immediately report all server security incidents on critical servers to OIS via e-mail sent to abuse@uc.edu. Please be sure to include as much information as possible.

3.6.1.2. Protect evidence pertaining to the incident. It is particularly important to preserve as much forensics data as possible.

3.6.1.3. If the server contains or is used to process Restricted Data, then unplug the network connection(s) to prevent data loss. You can remove network connectivity for other servers, but be aware that the intruders may have rigged things to damage the server on loss of network connectivity.

3.6.1.4. Await instructions from OIS.

   Note: If you feel this is a time sensitive matter, contact the UCIT Integrated Help Desk at 513-556-HELP (4357) and stress that "this is a security incident related contact and the proper contact from the UCIT Office of Information Security needs to be notified."

3.6.1.5. Do not kill running processes, disable running services, run anti-virus or anti-spyware scans, move, rename or delete files, or shut down, log into or reboot the system. Any changes you make to the system will obscure potentially valuable evidence.

3.7. Logging

3.7.1. Technical Staff MUST:

3.7.1.1. Configure systems to capture appropriate levels of information. Do not reduce audit levels below the vendor defaults; increase audit levels above the default settings where possible.

3.7.1.2. Log all configuration or file changes and system events in an audit log.
3.7.1.3. Retain all system logs for at least 90 days in a safe and secure manner, limiting all user write access to ensure log integrity.

3.7.1.4. Copy logs (in real time if possible) to a separate log server which is properly secured. This specifically includes UNIX syslog, Windows event logs, any security/authentication (successful and unsuccessful) logs, any separate application, web, email and database server logs, and DHCP logs. Also copy logs with specific utility in incident investigations to the log server.

3.7.1.5. Review the contents of system and application logs daily for unauthorized or unexpected activity and take appropriate action to resolve or report this activity if it deemed a security incident.

3.7.1.6. Ensure that all system times are standardized and that logs reflect those standardized time settings.

3.7.2. Technical Staff SHOULD:

3.7.2.1. Adopt automated log monitoring tools.

3.7.2.2. Contact OIS for information regarding log aggregation into the OIS Central Log Management System.

3.8. Accounts and Passwords

3.8.1. Technical Staff MUST:

3.8.1.1. Provide accounts with system administration capabilities to as few individuals as is necessary.

3.8.1.2. Change all domain and local administrative passwords every 90 days.

3.8.1.3. Provide all users with their own non-administrative logon accounts.

3.8.1.4. Prohibit use of administrator/root level accounts as logon accounts except when absolutely necessary. Administrators should use their own personal accounts to logon and then elevate their privileges as needed to do work (using tools such as UNIX “sudo”, Windows “runas” or “winsudo”).

3.8.1.5. Ensure all critical servers meet or exceed UC password complexity requirements as defined in the Password Policy.

3.8.2. Technical Staff SHOULD:

3.8.2.1. Evaluate strong authentication methods and adopt them whenever possible to protect critical university services and information. Examples of strong authentication include: two-factor authentication, one time password systems and restricted logins.

3.9. Internal Change Control Procedures

3.9.1. Technical Staff MUST:

3.9.1.1. Adopt change control procedures appropriate for the unit’s IT and business environments.

3.10. Secure Software Design, Implementation and Testing Procedures

3.10.1. Unit Administration MUST:

3.10.1.1. Ensure that application developers receive training to design, implement, and test secure code.

3.10.1.2. Ensure that all code is reviewed to identify common mistakes and fix code flaws to ensure that similar code sections are fixed.
3.11. Network and Firewalls

3.11.1. Technical Staff MUST:

3.11.1.1. Configure any remote access to critical servers from outside the DMZ or private network to use encrypted transport.
3.11.1.2. Log all access attempts to remote access end points (VPN concentrators, servers allowing Remote Desktop, Terminal Services, SSH, etc).
3.11.1.3. Monitor remote access logs DAILY for unauthorized activity.
3.11.1.4. Restrict remote access to defined external clients or servers and monitor the system for unauthorized activity.
3.11.1.5. Segregate critical and non-critical servers LAN segments.
3.11.1.6. Configure critical servers to synchronize their clocks with an accurate time source at least once a day using the university's existing NTP services.
3.11.1.7. Place servers behind a network-based firewall that blocks all inbound traffic by default. If unable to utilize a network-based firewall, an exception to this element must be filed by a Risk Acceptance Form with OIS.
3.11.1.8. Limit service exposure through firewall rules and controls and monitor them for unauthorized activity.

3.11.2. Technical Staff SHOULD:

3.11.2.1. Configure remote access to require strong authentication methods, either through one-time passwords, a two-factor system, or through TLS with client and server certificates.
3.11.2.2. Configure host-based firewalls to filter outbound traffic on the critical server using rules consistent with the department’s business requirements.

3.12. Service Configuration

3.12.1. Technical Staff MUST:

3.12.1.1. Disable unneeded or unnecessary services from running on the critical server. Eliminate default processes or services that do not support the operation of the server or its hosted applications.
3.12.1.2. Disable unneeded or unnecessary ports from running on the critical server.

4. Compliance

4.1. Standards Compliance

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

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 CSSS, 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 CSSS 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 will manage an up-to-date database of critical server information.

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 CSSS, 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** – computer system administrators responsible for the operation and management of systems and servers which store or provide access to institutional data.

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

**Data Steward** – university employees who have direct operational-level responsibility for information management.

**Data Trustee** – university administrators at the vice presidential level who bear the ultimate responsibility for ensuring the protection of the data stored by those in their reporting area.

**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 CSSS. 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 CSSS 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](#) as 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 CSSS 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

Asset Disposition Policy

9. Phone Contacts

| UCIT Office of Information Security | 513-558-ISEC (4732) |
| UCIT Integrated Help Desk          | 513-556-HELP (4357) |
Appendix A

Critical Server Security Standard
Evaluation Checklist for Critical Servers

A 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, UCIT 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><strong>Physical Security</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provide an appropriately secured environment to house critical servers that will prevent unauthorized entry, access or theft.</td>
<td>Must</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consider providing levels of environmental protection and monitoring that are commensurate with the risks and consequences of server failure due to loss of power, overheating, theft and other physical risks.</td>
<td>Should</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Backup and Recovery</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Follow best practices for backing up critical servers.</td>
<td>Must</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encrypt backup media including backup tapes that contain Restricted Data.</td>
<td>Must</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Securely store encryption keys necessary to decrypt the backups separately from the backup media.</td>
<td>Must</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Document key management procedures for decrypting backups and assure that they are available to more than one person and approved by the Data Custodian and Data Steward.</td>
<td>Must</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test and validate backup procedures work at least one time per year for all critical systems.</td>
<td>Must</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Data Destruction</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Properly sanitize and/or dispose of media containing Restricted Data when the data is no longer needed according to the Data Protection Policy and Asset Disposition Policy.</td>
<td>Must</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Follow the Surplus Equipment policies and procedures for proper reuse/recycling/disposal of university equipment.</td>
<td>Must</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Intrusion Detection and Security Tools</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Treat and investigate system changes as computer security incidents unless it can be determined conclusively that the changes were authorized.</td>
<td>Must</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implement host-based intrusion detection methods that incorporate baseline comparisons.</td>
<td>Should</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Install a file integrity monitoring system to monitor system changes.</td>
<td>Should</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Incident Response</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Immediately report all server security incidents on critical servers to the OIS via e-mail sent to <a href="mailto:abuse@uc.edu">abuse@uc.edu</a>. Please be sure to include as much information as possible.</td>
<td>Must</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protect evidence pertaining to the incident. It is particularly important to preserve as much forensics data as possible.</td>
<td>Must</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>If the computer contains or is used to process Restricted Data, then unplug the network connection(s) to prevent data loss. You can remove network connectivity for other computers, but be aware that the intruders may have rigged things to damage the computer on loss of network connectivity.</td>
<td>Must</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Await instructions from OIS. NOTE: If you feel this is a time sensitive matter, contact the UCIT Integrated Help Desk at 513-556-HELP (4357) and stress that “this is a security incident related contact and the proper contact from the UCIT Office of Information Security needs to be notified.”

<table>
<thead>
<tr>
<th>Must</th>
</tr>
</thead>
</table>

Do not kill running processes, disable running services; run anti-virus or anti-spyware scans, move, rename or delete files, or shut down, log into or reboot the system. Any changes you make to the system will obscure potentially valuable evidence.

<table>
<thead>
<tr>
<th>Must</th>
</tr>
</thead>
</table>

**Logging**

Configure systems to capture appropriate levels of information. Do not reduce audit levels below the vendor defaults; increase audit levels above the default settings where possible.

| Must |

Log all configuration or file changes, and system events in an audit log.

| Must |

Retain all system logs for at least 90 days in a safe and secure manner, limiting all user write access to ensure log integrity.

| Must |

Copy logs (in real time if possible) to a separate log server which is properly secured. This specifically includes UNIX syslog, Windows event logs, any authentication logs, any separate application, web, email and database server logs, and DHCP logs. Also copy logs with specific utility in incident investigations to the log server.

| Must |

Review the contents of system and application logs daily for unauthorized or unexpected activity and take appropriate action to resolve or report this activity if it deemed a security incident.

| Must |

Ensure that all system times are standardized and that logs reflect those standardized time settings.

| Must |

Adopt automated log monitoring tools.

| Should |

Contact OIS for information regarding log aggregation into the OIS Central Log Management System.

| Should |

**Accounts and Passwords**

Provide accounts with system administration capabilities to as few individuals as is necessary.

| Must |

Change all domain and local administrative passwords every 90 days.

| Must |

Provide all users with their own non-administrative logon accounts.

| Must |

Prohibit use of administrator/root level accounts as logon accounts except when absolutely necessary. Administrators should use their own personal accounts to logon and then elevate their privileges as needed to do work (using tools such as UNIX “sudo”, Windows “runas” or “winsudo”).

| Must |

Ensure all critical servers meet or exceed the OSU Password standard requirements.

| Must |

Evaluate strong authentication methods and adopt them whenever possible to protect critical university services and information. Examples of strong authentication include: two-factor authentication, one time password systems, restricted logins.

| Should |

**Internal Change Control Procedures**

Adopt change control procedures appropriate for the unit’s IT and business environments.

| Must |

**Secure Software Design, Implementation and Testing Procedures**

Ensure that application developers receive training to design, implement, and test secure code.

| Must |

Ensure that all code is reviewed to identify common mistakes and fix code flaws to ensure that similar code sections are fixed.

| Must |

**Network and Firewalls**

Configure any remote access to critical servers from outside the DMZ or private network to use encrypted transport.

| Must |

Log all access attempts to remote access end points (VPN concentrators, servers allowing Remote Desktop, Terminal Services, SSH, etc.).

| Must |

Monitor remote access logs DAILY for unauthorized activity.

| Must |

Restrict remote access to defined external clients or servers and monitor the system for unauthorized activity.

| Must |

Segregate critical and non-critical servers LAN segments.

| Must |

Configure critical servers to synchronize their clocks with an accurate time source at least once a day using the university’s existing NTP services.

| Must |

Place servers behind a network-based firewall that blocks all inbound traffic by default. If unable to utilize a network-based firewall, an exception to this element must be filed by a Risk Acceptance Form with OIS.

<p>| Must |</p>
<table>
<thead>
<tr>
<th><strong>Limit service exposure through firewall rules and controls and monitor them for unauthorized activity.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service Configuration</strong></td>
</tr>
<tr>
<td>Disable unneeded or unnecessary services from running on the critical server. Eliminate default processes or services that do not support the operation of the server or its hosted applications.</td>
</tr>
<tr>
<td><strong>Compliance</strong></td>
</tr>
<tr>
<td>All designated critical devices must comply with the CCSS and CSSS.</td>
</tr>
<tr>
<td><strong>In cases where it is not possible to bring a device into compliance</strong></td>
</tr>
<tr>
<td>Units or individuals must employ compensating controls.</td>
</tr>
<tr>
<td>Units must document compensating controls and must retain this documentation for audit so long as the device is in operation.</td>
</tr>
<tr>
<td>Units must request an exemption to one or more elements of the standard if no compensating control is possible.</td>
</tr>
<tr>
<td>Risk Acceptance Form must be submitted to OIS</td>
</tr>
<tr>
<td><strong>Registration of Critical Servers</strong></td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td><strong>Compliance Mechanisms</strong></td>
</tr>
<tr>
<td>When tools that perform automated detection of patches and vulnerabilities are available, units should regularly inspect their networks to gather information regarding the state of compliance.</td>
</tr>
<tr>
<td>When tools that perform automated detection of patches and vulnerabilities are not available, units should consider purchasing/acquiring these tools.</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>