Client Computing Security Standard (CCSS)

1. Background

The purpose of the Client Computing Security Standard (CCSS) is to (a) help protect each user's device from harm, (b) to protect other users' devices from harm, and (c) to protect the University of Cincinnati's (UC) data network and its allied resources from misuse. The CCSS consists of four requirements, all of which must be met before using a device on UC's network:

1.1. The device must use firewall software if technically possible. This helps protect the user's device from external intrusions.

1.2. Software on the device must be current. This is particularly important for high-risk software, such as the operating system and web browser. Staying current makes the user's device less vulnerable to outside subversion, helping to protect the device and its data.

1.3. The device must have software that helps guard against malicious or undesired software such as viruses, spyware or adware and this protection must be kept up-to-date per industry standards. Collectively, this anti-malware helps defend the user's device and helps prevent it from being used to exploit other's devices.

1.4. The device must have a user name and password or other sign-on mechanism that helps prevent its use by unauthorized individuals. Each user must have a unique user name used only by that user. The password must meet the requirements as defined in the Password Policy.

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

In addition to the CCSS 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 Policy.

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.

> ***Note:*** *for the purposes of this standard, the term "computer" is interchangeable with "device". Devices include any network connectable item, including items such as any fixed or portable computer, laptop, tablet or handheld 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.*

2. Implementation Guidance

Since the scope of the CCSS 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 IT@UC Office of Information Security (OIS) at infosec@uc.edu.

3. The Client Computing Security Standard

3.1. Each device must meet the following minimum standards while connected to UC's network:

3.1.1. The device must be guarded by an up-to-date and active host-based firewall set to protect it from unauthorized network traffic.

3.1.2. Supported operating system and application software with current security patches must be installed.

3.1.3. The device must be protected against malicious or undesired software such as viruses, spyware or adware and this protection must be kept up-to-date per industry standards.

3.1.4. Access to the device must require appropriate authentication controls such as unique account identifiers and robust passwords as defined in the Password Policy.

3.2. Academic, administrative and support units (referred to as "units" from here on) must develop and maintain processes, practices or tools to ensure initial and continued compliance on university owned/managed devices with the standard

requirements either manually or automatically.

> ***Note:*** *Units must develop processes, practices or tools to quarantine or disconnect any non-compliant device until it is brought into compliance.*

3.3. Passwords may not be shared with others and must be changed periodically not to exceed a 180 day cycle. All university owned/managed devices must meet or exceed the university password requirements including complexity and password life-cycle qualities as defined in the Password Policy. Generic and "Guest" accounts are prohibited and must be disabled. Any manufacturer delivered accounts must be deactivated when technically possible and those with well-known passwords must be changed.

3.4. In some cases it may not be possible to bring a device 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. Units must document compensating controls and must retain this documentation for audit so long as the device is in operation.

Units must request an exemption to one or more elements of the standard if no compensating control is possible. For example, a generic user account may be required for a public workstation instead of a named user logging into the machine. All exemptions must be documented via a Risk Acceptance Form which must be submitted to OIS who will review and approve or deny the requests.

> ***Note:*** *Devices 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.*

3.5. Units may specify additional standards or requirements within their administrative areas of responsibility. Units must document and publish any additional requirements, preferably on the unit's web site. These additional requirements must be reviewed annually and should be modified as needed. The unit's additional standards may strengthen or extend but may not weaken the provisions of the CCSS.

4. Compliance

4.1. Roles of Units, IT staff, and others

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

The user is responsible for compliance on personally owned devices.

Users granted responsibility for administration on university equipment will share responsibility for compliance with local IT staff (i.e. local administrator rights, users granted access via a local administrative privilege.) See the Local Administrative Privilege Standard (LAPS) for additional information.

Users who do not comply with this standard are in violation of the Data Governance & Classification Policy, Vulnerable Electronic Systems and/or Acceptable Use of University Information Technology Resources. 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.

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

OIS is tasked with the responsibility of maintaining the CCSS 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 devices to

determine overall compliance.

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

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

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 complete a Risk Acceptance Form. Only upon approval of the Risk Acceptance Form may the device 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.

Anti-malware – reactive software designed to combat malware software (malicious or undesired software such as viruses, spyware or adware) by protecting computers from attack, neutralization or removal of the offensive programs. The anti-malware software typically uses updates commonly referred to as "definitions" to update the database of undesired software signatures.

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 theRisk 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 CCSS, 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).*

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

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 CCSS. 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 then that firewall must be enabled to satisfy the CCSS requirement.

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"

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 CCSS 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.

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 owned/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. University managed devices typically are not owned by the university, but are used for university business and supported by university staff.

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. Related links

Security Standards

Data Governance & Classification Policy

Vulnerable Electronic Systems

Acceptable Use of University Information Technology Resources

8. Contact Information

IT@UC Office of Information Security 513-558-ISEC (4732)

Email: infosec@uc.edu

9. History:

Issued: 12/15/2014
Revised: 3/25/2016
Revised:3/21/2017

Appendix A

Client Computing Security Standard Evaluation Checklist

Statement	Must or Should?	Met	Not Met	Comments
Before using a computer on UC's network, users must comply with the Data Governance & Classification Policy, the Vulnerable Electronic Systems Policy and the Use of Information Technology Policy.	Must			
Complies with Client Computing Security Standard (CCSS).	Must			
While Connected to UC's Network				
The device must be guarded by an up-to-date and active host-based firewall set to protect it from unauthorized network traffic.	Must			
Supported operating system and application software with current security patches must be installed.	Must			
The device must be protected against malicious or undesired software such as viruses, spyware or adware and this protection must be kept up-to-date per industry standards.	Must			
Access to the device must require appropriate authentication controls such as unique account identifiers and robust passwords as defined in the Password Policy.	Must			
Compliance Process				
Units must develop and maintain processes, practices or tools to ensure initial and continued compliance on university owned/managed devices with the standard requirements either manually or automatically.	Must			
Units must develop processes, practices or tools to quarantine or disconnect the non-compliant device until it is brought into compliance.	Must			
Accounts and Passwords				
Passwords may not be shared with others.	Must			
All university owned/managed devices must meet or exceed the university password requirements including complexity and password life-cycle qualities as defined in the Password Policy.	Must			
Generic and "Guest" accounts are prohibited and must be disabled. Any manufacturer delivered accounts must be deactivated when technically possible and those with well-known passwords must be changed.	Must			
In cases where it is not possible to bring a device into compliance				
Units or individuals must employ compensating controls.	Must			
Units must document compensating controls and must retain this documentation for audit so long as the device is in operation.	Must			
Units must request an exemption to one or more elements of the standard if no compensating control is possible via a Risk Acceptance Form.	Must			
Risk Acceptance Form must be submitted to OIS.	Must			
Units may specify additional standards or requirements within their administrative areas of Responsibility				
Additional requirements, if any, must be documented and published by the unit, preferably on the unit's web site.	Must			
Additional requirements, if any, must be reviewed annually and should be modified as needed. The unit's additional standards may strengthen or extend but may not weaken the provisions of the CCSS.	Must			
Compliance Mechanisms				
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.	Should			
When tools that perform automated detection of patches and vulnerabilities are not available, units should consider purchasing/acquiring these tools.	Should			

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.	Should		
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.	Must		
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.	Must		