UNIVERSITY
OF
CALIFORNIA

UCOP
ITS
Systemwide CISO Office
Systemwide IT Policy

UC Secure Software Configuration Standard

Revision History

Date:	By:	Contact Information:	Description:
04/02/18	Robert Smith	robert.smith@ucop.edu	Approved by the CISOs for consideration by ITLC and shared governance. Interim until approved by ITLC.
8/1/2019	Robert Smith	robert.smith@ucop.edu	Updated based on comments from Locations. No requirements were added or removed. Clarifications made in sections 1, 4.2.18 and 4.2.25. Added cross-referencing to UC's Secure Software Development Standard.
9/10/19	Robert Smith	robert.smith@ucop.edu	Updated to conform to standard style sheet and to use consistent terms for portable media.
10/3/19	Robert Smith	robert.smith@ucop.edu	Approved by the ITLC.

Contents

1 Background and Purpose 3
2 Scope 3
3 Definitions and Key Terms 3
4 Requirements for Secure Software Configuration 3
4.1 General requirements 3
4.2 Secure software configuration practices 4
4.2.1 General options 4
4.2.2 Secure communication protocols 4
4.2.3 TLS 5
4.2.4 Digital certificates 5
4.2.5 Default credential/account removal 5
4.2.6 File access and cloud access to files and information 5
4.2.7 Local and cloud access to administrative consoles and instance management 5
4.2.8 Anonymous connections 5
4.2.9 Component-specific credentials of service accounts 6
4.2.10 Application credential encryption 6
4.2.11 User authentication 6
4.2.12 Service/machine accounts 6
4.2.13 Supplier remote access 6
4.2.14 Setting session timeout 6
4.2.15 Separate applications and databases 6
4.2.16 Operating systems – current version and patching 7
4.2.17 Other software – current version and patching 7
4.2.18 Development and test systems 7
4.2.19 Using the proper network 7
4.2.20 Character set selection (encoding) 7
4.2.21 Log file management 7
4.2.22 Hardening 7
4.2.23 Database – TDE 7
4.2.24 Encryption at rest 7
4.2.25 Backup and archival 7
4.2.26 Security Agents 8
4.2.27 APIs, interfaces and data transfers 8
5 References 8
6 Appendix A – Other Considerations 9

1 Background and Purpose

This Standard defines the requirements for the secure configuration of purchased, leased, open source, in-house developed or cloud-based applications that are configured by a Unit or Service Provider. These are sometimes called "commercial-off-the-shelf software" (CoTS) or "software-as-a-service" (SaaS).

This Standard must be used in conjunction with UC's information security policy, BFB-IS-3 Electronic Information Security and UC's Secure Software Development Standard.[1]

As outlined in IS-3, security is part of the overall system lifecycle. Applications and cloud services are often not secure by default and thus require specific steps to achieve a secure outcome.

Full-featured and robust applications, if misconfigured, can weaken cyber defense. Proper configuration is therefore required to ensure adequate cyber risk management.

All applications, regardless of how acquired, can represent significant cyber risks (e.g., free, open-source, cloud offerings, SaaS, downloaded, licensed, etc.). It is important to configure both free and purchased applications properly. Units should also note that a company's size, longevity and prestige do not indicate the effectiveness of its ability to manage cyber risk. Many Suppliers focus on getting applications to run well with a minimum investment of time and without concern for ongoing support costs. The best time to start applying good security principles is before acquisition of an application or during the selection process of a Supplier (such as a cloud server or SaaS).

Units should use this Standard to guide the configuration of all of their applications in order to manage cyber risk.

2 Scope

This Standard applies to all Locations, and to all purchased, leased, open source, in-house developed or cloud-based applications that are configured by a Unit or Service Provider.

The UISL (Unit Information Security Lead) and assigned IT Workforce Members are responsible for meeting the requirements in this Standard.

3 Definitions and Key Terms

For more information about definitions, consult the IT Policy Glossary.

4 Requirements for Secure Software Configuration

Software containers can be layered (e.g., a database running on an operating system) and are often co-located or shared (e.g., multiple applications sharing database servers). Thus, all software containers must be securely configured regardless of the individual Protection Level (PL) designation.

4.1 General requirements

This section describes basic requirements that apply to all applications.

[1] Other standards will often apply to developed software, customizations and extensions (e.g., Event Logging Standard, Account and Authentication Management Standard, Security Key and Certificate Management Standard, etc.).

IT Workforce Members must:

- Select and use Suppliers who can adequately secure Institutional Information.
- Ensure Supplier agreements are in compliance with IS-3 Section III, subsection 17.
- Plan and budget for supporting security tools to manage cyber security risk and implement required compensating controls.
- Establish, document and maintain a security plan for each application.
    - Set requirements for business processes (e.g., transaction logging, transaction monitoring and tying actions to a specific user, which is also known as nonrepudiation).
    - Consider requirements mandated by other security controls (e.g., interfaces to other logging and monitoring or data leakage detection systems).
- Design security into all architectural layers (e.g., business, data, applications and technology).
- Analyze new and existing technology to determine security risks and review design against known attack patterns.
- Regularly review engineering procedures to ensure they keep pace with new threats and technological advancements.
- Create a request and approval process for business users and privileged/technical users by applying the least-privilege method.
- Inform users and operators of roles and responsibilities.
- Implement security controls based on the Protection Levels identified in IS-3.
- Plan and conduct regularly a review of security logs and security configuration settings based on risk.

4.2 Secure software configuration practices

4.2.1 General options

IT Workforce Members must configure software so that:

- Appropriate security controls are enabled.
- Auditing features are enabled and provide information to support the detection of malicious action.
- The application is resistant to compromise.

Tip: Cloud service providers, resellers/dealers/VARS and application providers often prioritize the speed of implementation and the reduction of support costs over ensuring the highest level of security. Never assume applications or services are secure by default. Some software can be costly to secure, so it is important to investigate its level of security before acquiring it.

4.2.2 Secure communication protocols

IT Workforce Members must disable unencrypted protocols when encrypted protocols are available (e.g., disable HTTP when HTTPS is available).

Institutional Information classified at Protection Level 3 or higher must be transmitted using secure protocols.

Tip: See EAA-070 HTTPS Everywhere and EAA-061 Secure Data Transfer Mechanisms for technical details and guidance.

4.2.3 TLS

IT Workforce Members must use TLS 1.2 or later for communication when:

- Credentials are being exchanged.
- Institutional Information classified at Protection Level 3 or higher is transmitted.

IT Workforce Members must select a CISO-approved strong cipher suite for TLS.

IT Workforce Members must force HTTPS (e.g., no HTTP connections).

4.2.4 Digital certificates

IT Workforce Members must use a certificate authority-signed certificate (e.g., no self-signed certificates).

4.2.5 Default credential/account removal

IT Workforce Members must, when possible, remove or disable user or machine credentials and/or accounts that are provided "out-of-the-box." These are often known as a default user name and password.

If a specific account must be used (e.g., root, appname, appuser, etc.), the responsible IT Workforce Member must change the default password/passphrase, use a strong passphrase and enforce multifactor authentication if the login/authentication service is available on a public network.

Note: See the UC Account and Authentication Management Standard for additional information about securing accounts.

4.2.6 File access and cloud access to files and information

IT Workforce Members must ensure other Workforce Members understand and set file sharing and cloud access controls and features so that only intended parties have access to Institutional Information.

Tip: Many data breaches are caused by incorrect file sharing or cloud security settings. File shares and cloud applications may or may not be secure by default. Care is required. Users can often make setting changes or use features like "anyone with a link can edit" that expose sensitive data. In many cases, adding a type of product or layer called a "cloud access security broker" is a prudent step in the ongoing process of managing cyber risk.

4.2.7 Local and cloud access to administrative consoles and instance management

IT Workforce Members must understand and set local and cloud access controls and features so only intended parties have access to configuration options.

For on premise remote access and for cloud software that is storing, processing or transmitting Institutional Information classified at Protection Level 3 or higher, multifactor authentication must be used.

4.2.8 Anonymous connections

IT Workforce Members must ensure that a configuration allowing anonymous connections only does so for applications hosting Institutional Information classified at Protection Level 1.

IT Workforce Members must remove or disable unauthenticated access for applications hosting Institutional Information classified at Protection Level 2 or higher.

4.2.9 Component-specific credentials of service accounts

IT Workforce Members must create unique service account credentials for each logical part of the software/system.

Using the same credential for a database and application server is prohibited. The application must have one user name and passphrase and the database must have another user name and passphrase.

4.2.10 Application credential encryption

IT Workforce Members must ensure that application credentials are encrypted both when stored and while in transit.

Note: Modern web servers have tools to store application credentials securely. This method often requires encrypting the configuration. Units should never try to implement their own schemes and must use proven off-the-shelf methods for protecting credentials. Each technology has specific guides for secure implementation.

4.2.11 User authentication

Units must use a CISO-approved method for authenticating users to applications.

4.2.12 Service/machine accounts

IT Workforce Members must ensure that:

- They do not use service/machine accounts.
- Service/machine accounts comply with the UC Account and Authentication Management Standard.

4.2.13 Supplier remote access

IT Workforce Members must secure Supplier remote access with multifactor authentication and unique credentials.

Tip: Supply chain compromise is one of the most common tactics used by attackers. Many Suppliers optimize based on their convenience and not the security of the client.

4.2.14 Setting session timeout

IT Workforce Members must set application session time-outs to the approved values.

4.2.15 Separate applications and databases

IT Workforce Members must install public facing applications storing Institutional Information classified at Protection Level 3 or higher so that the database server is logically separated from the application server.

Tip: This may require a custom installation or setup. “All-in-one” installations are not appropriate for public-facing software, systems or applications storing Institutional Information classified at Protection Level 3 or higher.

4.2.16 Operating systems – current version and patching

IT Workforce Members must make sure that operating systems and the patching of operating systems comply with the UC Minimum Security Standard.

4.2.17 Other software – current version and patching

IT Workforce Members must make sure that other software and the patching of other software comply with the UC Minimum Security Standard.

4.2.18 Development and test systems

IT Workforce Members must configure and secure test development systems to protect production systems, Institutional Information and credentials.

4.2.19 Using the proper network

IT Workforce Members must place systems on the approved Location network and one designed for the appropriate protection of the Institutional Information and IT Resources.

4.2.20 Character set selection (encoding)

IT Workforce Members must set software configuration options for encoding to use UTF-8 or a standard character set for which full input validation can be performed.

4.2.21 Log file management

IT Workforce Members working with software that is processing or storing Institutional Information classified at Protection Level 3 or higher must comply with the UC Event Logging Standard.

4.2.22 Hardening

IT Workforce Members must execute recommended hardening scripts for software and for operating systems processing or storing Institutional Information classified at Protection Level 3 or higher or Availability Level 3 or higher.

4.2.23 Database – TDE

IT Workforce Members must enable Transparent Data Encryption (TDE) capabilities or similar for databases storing Institutional Information classified at Protection Level 3 or higher.

- Whole database/schema/tablespace encryption is required.
- Column level encryption requires approval via an exception request.

4.2.24 Encryption at rest

IT Workforce Members must enable encryption at rest capabilities for Institutional Information classified at Protection Level 3 or higher.

4.2.25 Backup and archival

IT Workforce Members must establish, implement and test a backup and archival process that:

- Encrypts any Institutional Information classified at Protection Level 3 or higher when stored on portable media.
- Meets the record retention schedule.
- Meets the business continuity requirements described in BFB-IS-12.

4.2.26 Security Agents

IT Workforce Members must install and enable Location- or Unit-required security agents.

Note: Security agents can include anti-malware, logging, data loss prevention, host firewall, host intrusion detection and compliance tools.

4.2.27 APIs, interfaces and data transfers

IT Workforce Members must enable secure transmission and authenticated protocols for interfaces transmitting Institutional Information classified at Protection Level 3 or higher when on public or mixed Protection Level networks.

Note: For more on this topic, see EAA-061 Secure Data Transfer Mechanisms.

Note: Protect and manage API keys like other secrets. Use cryptographically strong keys and consult the UC Encryption Key and Certificate Management Standard. The correct use and application of API keys is important to manage cyber risk. Consult the CISO for help.

Tip: Software and applications often have easy to use features that export data to a variety of formats and through a variety of interfaces. Often these must be secured separately. Reporting servers/add-ons is an example. Institutional Information can leak if these are not secured.

5 References

UC Policy

Business and Finance Bulletin IS-3 – Electronic Information Security

Business and Finance Bulletin IS-12 – Continuity Planning and Disaster Recovery

UC Standards

IT Security Committee – UC Minimum Security Standard

IT Security Committee – UC Account and Authentication Management Standard

IT Security Committee – UC Secure Software Development Standard

External Resources

Center for Internet Security, Critical Security Controls, https://www.cisecurity.org/controls

Open Web Application Security Project (OWASP), https://www.owasp.org

6 Appendix A – Other Considerations

There are some other important information security considerations for software and applications using public networks. Units should consider implementing the following tasks:

- Assess the level of confidence each party requires in each other's claimed identity (e.g., through authentication).
- Ensure there is an agreement and documentation clearly explaining the authorization processes in place regarding individuals allowed to sign key transactional documents, issue these documents and/or approve their contents.
- Avoid loss or duplication of transactional information.
- Evaluate liability associated with any fraudulent transactions.