University of Colorado Boulder	**University of Colorado Boulder** **Campus IT Standard**

Effective:	March 1, 2016
Responsible Office:	The Office of the AVC for IT and CIO
Title:	Identification and Management of Security Flaws in IT Systems
Approved:	Larry Levine

Purpose:

Information systems that are connected to the University of Colorado network run the risk of compromise, which may lead to a breach of confidentiality or misuse of those systems and/or the University of Colorado network. This standard defines a means by which vulnerable and/or compromised systems or applications might be identified and isolated from the University of Colorado network or internet pending correction of the problem.

A. Introduction

All devices connected to the University of Colorado at Boulder network, regardless of ownership or operation, are subject to security vulnerability scanning and/or penetration testing to be conducted by the IT Security Office. Network, system, and application performance and/or availability may be affected by the network scanning. Arrangements with the IT Security Office for exceptions (requests to not scan a device or application) can be made if vulnerability testing interferes with academic or research applications and other security measures (e.g., network filtering, firewall, etc.) are in place to mitigate risk. Any requests must be submitted to the IT Security Office for review and approval. Exception requests must include:

- Why the scanning exception is being requested.
- Risk to the enterprise of not scanning the device.
- Mitigation controls that have been implemented, and date of implementation.

The IT Security Office is the authorized entity to perform campus-wide network scanning of all University of Colorado at Boulder computer systems. Departmental system administrators may scan systems in their area of responsibility in coordination with the IT Security Office to avoid confusion with unauthorized intrusion attempts.

When a security flaw has been identified, the IT Security Office will restrict access to the vulnerable systems. Before restricting access the IT Security Office shall consider the risk of the vulnerability,

sensitivity of data processed on the vulnerable system, and the impact to University operations to determine the appropriate actions to protect University information and information systems.

B. Policy

Vulnerability assessment frequency

- High-risk systems[1]: systems that are not managed by OIT will be scanned, at minimum, quarterly using network vulnerability scans and private data scans. If a host vulnerability scan reveals that a web service is running, a scan using web application vulnerability tools will follow. Systems included as high-risk are:
    - Internet-facing systems: Systems with an unrestricted IP exception at the campus border firewall
    - Confidential or highly confidential data systems1: Systems identified as storing, transmitting, or processing information assets classified as private. A vulnerability scan using a username and password may be required by law, regulation, or standard for this type of system.
    - Hosts subject to Payment Card Industry Data Security Standards will must have a vulnerability scan completed quarterly. Scans will be configured to perform checks using system credentials.
- OIT-managed systems: systems that are under the direct operation or responsibility of the Office of Information Technology staff will be scanned according to a schedule, interval, and level agreed upon by the IT Security Office and OIT operations and/or OIT desktop support.
- All other systems: systems that are not categorized as high-risk or OIT-managed will be scanned within 48 hours of discovery on the University of Colorado's network and, at minimum, annually or spontaneously when a high risk network propagating malware has been reported thereafter.

Vulnerability remediation expectations

Expected timeframes for completion of remediation will vary based on the data criticality and sensitivity of the system and the criticality of the vulnerability. The following expectations apply for low impact systems which are accessible from the Internet:

- Confirmed Urgent Vulnerability (level 5) with serious known exploit – 48 hours to remediate
- Confirmed Urgent Vulnerability (level 5) - 14 days to remediate
- Confirmed Critical Vulnerability (level 4) – 30 days to remediate

If remediation is not completed within the expected time or a risk acceptance decision (following the process in section D below) is not completed, then it will be necessary to block access from the Internet until remediation is complete. If the IT Security Office does not receive a response to the initial notification of the vulnerability it may be necessary to block access from the Internet until remediation is complete.

The following expectations apply for high-risk systems (e.g., PCIDSS or systems maintaining highly-confidential data):

- Confirmed Urgent Vulnerability (level 5) – Business must be suspended until remediated.

---

[1] Impact and data classification definitions are based on the CU data classification process http://www.cu.edu/sites/default/files/CUdataclassification.docx

- Confirmed Critical Vulnerability (level 4) – Business must be suspended until remediated.
- Confirmed Serious Vulnerability (level 3) – Action plan submitted to campus ISO with remediation occurring within 180 days. If found on 3 plus consecutive plans, campus ISA and treasury will be notified for possible suspension.

If remediation is not completed within the specified time network access may be revoked. In the case of PCIDSS systems the campus ISA and University Treasury will determine if the merchant account is to be suspended.

The IT Security Office will confirm remediation with a verification scan one day after the expected timeframe for completion.

C. Administration and Enforcement

The campus IT Security Office shall oversee the administration of this policy. Violations of policy will be referred to employee supervisor and/or departmental director as appropriate. The Associate Vice Chancellor for IT will be notified of policy violations to determine if it is necessary to shut down IT operations or transfer management of those operations to a service provider with requisite capabilities.

A vulnerability scan by the IT Security Office is required before a firewall exception is approved.

System and application administrators are responsible for assessment and application of security patches that impact systems under their management and supervision.

D. Exceptions

Exceptions to this policy will be treated as risk acceptance decisions and follow the CU Office of Information Security process

E. Definitions

- Vulnerability - a weakness or flaw in the security of an IT system that can be exploited to allow unauthorized access or use.
- Compromise - a vulnerability that has been found and exploited by an unauthorized user.
- Vulnerability Scanning - systematic attempts to identify weaknesses in a system or application in order to mitigate or correct the weakness before it is exploited.

- Vulnerability Severity Levels[2]:
  - Urgent (level 5) - Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.
  - Critical (level 4) - Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host

[2] Adapted from Qualys https://qualysguard.qualys.com/qwebhelp/fo_help/knowledgebase/vulnerability_levels.htm

- Serious (level 3) - Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.

F. Selected References to University Policies.

Information Security Program - http://www.cu.edu/ope/aps/6005

CU Risk Acceptance Process - http://www.cu.edu/sites/default/files/Information-Risk-Acceptance-Process-CJ.doc

G. Contact Information

Questions should be directed to Dan Jones, 303.735.6637 or mailto:dan.jones@colorado.edu