| Colorado<br>University of Colorado at Boulder | **CIO Campus-wide Policy** |
|---|---|

**Effective:** March 13, 2007
**Responsible Office:** CIO
**Policy Title:** Security of IT Resources Through Authentication, Registration, and Routing Procedures for Email Servers
**Approved** *IT Council*
**Purpose:** Outlines requirement for campus email servers

---

## A. Introduction:

CU-Boulder expects all IT personnel to maintain a secure IT environment that supports the needs of the teaching and research mission of the campus. In order to effectively accomplish this, IT personnel must take appropriate measures to manage the security of email servers.

## B. Policy Statement:

CU-Boulder requires all email servers to be registered with ITS on an annual basis through processes defined by the campus IT Security Principal. This process requires administrative oversight by the Organizational Unit (OU) director as defined in the IT Security Program APS. Registration is required for all servers connected to the CU-Boulder network or servers using a colorado.edu address.

CU-Boulder requires all email servers to route traffic through the central campus email router and SPAM/Virus gateway. In addition, all email connections are required to be authenticated connections as outlined in the CU-Boulder Minimum System Security Standards Policy. Exceptions to these two requirements will be determined by the campus CIO. The campus IT Security Principal will advise the campus CIO regarding policy exception risks.

## C. Responsibilities of Departments Maintaining Email Server(s):

1. Register all email servers[1] on an annual basis with current contact information.
2. Either provide contact information and access to appropriate network administrator or local support provider who would be available 24/7 to receive information regarding operational and/or security concerns, or accept the risk of the email server being taken off the CU-Boulder network until remediated if a compromise or vulnerability has been detected, which jeopardizes the campus network.
3. Configure email servers to route through the central campus email router and SPAM/Virus gateway.
4. Comply with the CU-Boulder Minimum Security Standards Policy as well as all applicable university, state and federal laws, policies, and regulatory requirements (see links below).

## D. Responsibilities of ITS:

1. ITS will provide a registration process for email servers.

---

[1] These servers will be subject to frequent security scans. If a security risk is identified the department will be notified to remediate vulnerabilities. Depending on the severity of the risk, the IT Security Principal has the authority to isolate the email server until the remediation is complete and verified by the campus IT Security Office. The department is required to perform remediation activities in the event of a detected vulnerability or compromise.

2. ITS will work with campus IT governance groups to develop appropriate services and requirements for SPAM handling and email routing that meets specialized needs.
3. ITS will provide guidance to departmental IT service providers who are undertaking remediation steps for email servers that have been identified with a vulnerability or compromise.

**E. Responsibilities of OUs:**

1. OUs (e.g. vice chancellors of administrative units, deans, department heads, etc.) have overall, local responsibility for the IT services within their area. This includes identifying the appropriate network administrator or local support provider who will ensure necessary security over the IT resources under their control.
2. OUs are responsible for continuity over the IT resources (e.g., by ensuring that change in employment does not result in the abandonment or mismanagement of IT devices attached to the network.)

**F. Enforcement:**

Any unregistered email servers will be blocked from the CU-Boulder network. Suspected violations to this policy will be referred to the CIO office.

**G. References to Applicable Polices:**

University of Colorado:

- IT Security in Personnel Job Descriptions, Responsibilities, and Training https://www.cusys.edu/policies/General/IT-Sec_Personnel-Job-Desc.pdf NEW - 1.1.07
- IT Security in University Operations, Continuity, and Contracting https://www.cusys.edu/policies/General/IT-Sec_UnivOps.pdf NEW - 1.1.07
- IT Security Program, https://www.cusys.edu/policies/General/IT-Sec_Prog.pdf NEW 1.1.07
- IT Resources User Responsibilities https://www.cusys.edu/policies/General/IT-ResourceUserResp.pdf NEW 1.1.07

University of Colorado at Boulder:

- Use of CU-Boulder's Computing and Network Resources http://www.colorado.edu/policies/cnr/index.html

ITS:

- Minimum Security Standards http://www.colorado.edu/its/security/csrweb.html

Federal Regulations:

- Federal Civil Procedure Rules 34, 37. and 45 concerning the discovery of electronically stored information: http://www.supremecourtus.gov/orders/courtorders/frcv06p.pdf and http://judiciary.house.gov/media/pdfs/printers/109th/31310.pdf