Appendix B

**REQUEST TO ACCESS ELECTRONIC COMMUNICATIONS OF OTHERS**

Our department requests authority to access electronic communications sent to an individual as described below:

1. Name, Title, and Department of person whose communications would be accessed:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Name & Title

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Department

2. Name, Title, and Department of person who will do the accessing:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Name & Title

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Department

3. Reason for access request:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4. What forms of communication will be accessed (e.g. E-Mail, Documents of File Servers)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

5. How long should the special access last? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

6. What will be done with the accessed messages? With whom will they be shared?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

7. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Signature of Requesting Department Chairperson or Unit Director

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Date

8. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Signature of Approving Dean or Vice Chancellor

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Date

9. Upon approval, this form is to be delivered to the following person as authorization for them to implement the requested special access.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Name & Title

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Department

**User Expectations**

The University may access and disclose employee or student individual content when the University deems a legitimate and appropriate business need and those instances are documented and approved by the appropriate authorities. In those instances, if it is necessary to access individual content on IT resources without the consent of an individual currently affiliated with the University, approval must be obtained from the appropriate authority or his or her designee. In the case of faculty and staff working in a school or college, this is the Dean; for all other staff, the Divisional Vice Chancellor; for undergraduate student users, the Dean of Students; and for graduate students, the Dean of the Graduate School. Individual content may be accessed without the consent of the user to comply with legal requirements (including, but not limited to, subpoena, court order, e-discovery request, and/or open records request) as determined by University Counsel. Departmental supervisors may request access to individual content when an employee retires, is terminated, unexpectedly passes away, or otherwise leaves the employment of the University.

If emergency access to individual content without the consent of the users is required to preserve public health and safety, or preserve the integrity of IT resources and campus facilities, notice shall be provided to the campus IT security principal, notifying them of the need to access files. The campus IT security principal can also assist in obtaining files. All instances of access will be logged by the IT security principal.

Individual content may be accessed through automated information security systems (such as antivirus software, intrusion detection systems, and/or data loss prevention systems) for the purposes of detecting and responding to threats to campus information resources. Excluding client antivirus or antimalware software, the campus IT security principal must authorize all automated information security systems that systematically access individual content. Automated information security systems will log only individual content needed to respond to and identify incidents.

Other than backups for disaster recovery purposes CU-Boulder does not systematically archive contents of email communications. CU-Boulder, at the direction of University Counsel, arranges ongoing archival of email accounts as required to meet legal requirements.

Reference:
<http://www.colorado.edu/policies/acceptable-use-cu-boulder%E2%80%99s-it-resources>