University of Oregon
Information Services
Exchange Administrator Authorization Form

Name: _________________________________  UO ID: ________________  Telephone: ____________
Department: ________________________    Job Title: ________________________  Email: ________________
Organizational Unit: __________________________________________________________
Dean or Department Head (printed name): _______________________________________
Dean or Department Head (signature): ____________________________  Date: ________________

NOTE: Exchange Administrator roles are reviewed annually and may be reassigned

Exchange Administrator Roles and Responsibilities

Departmental Exchange Administrators are granted full control of the calendars and electronic communications transmitted by users within their administrative area (OU). Exchange administrators have full control of all mailboxes including the ability to add and delete messages permanently without the knowledge of the user.

1. Access rules

A limited number of Information Services staff are granted access to modify email accounts for users. In addition, selected IT employees may be designated as Exchange Administrators and provided this access after approval and training from Information Services.

Staff with access to Exchange Mailboxes may not delegate or share their access with others – if an Exchange Administrator is out of the office, users must go to Information Services Help Desk for Exchange troubleshooting.

2. Auditing

All Exchange Administration actions are audited in the Microsoft Exchange system. Periodic reports will be run to review Exchange account modification. Information Services reserves the right to revoke access if misuse is detected.

3. Revocation

Violation of access rules may result in immediate revocation of access and may lead to disciplinary action, including dismissal. Violations may also lead to criminal and civil liability.
UO Code of Responsibility for Security and Confidentiality of Records and Files

Security and confidentiality are matters of concern to all University employees and to all other persons who have access to administrative records, education records, reports, or any other confidential or privileged documents or information. The purpose of this code is to clarify responsibilities in these areas. Each individual who has access to confidential or privileged information is expected to adhere to the regulations stated below.

Any person who has access to administrative records, education records, reports, or any other confidential or privileged documents or information, may not:

♦ Reveal the content of any record or report to anyone, except in the proper conduct of his or her work assignments and in accordance with University policies and procedures.
♦ Make or allow any unauthorized use of information.
♦ Include false, inaccurate or misleading entry in any report or record.
♦ Expunge a data record or a data entry from any record, report or file.
♦ Share individual passwords with any other person.
♦ Seek personal benefit or allow others to personally benefit from the knowledge of any confidential or privileged documents or information.
♦ Remove any original or copy of an administrative record, education record, report, or any other confidential or privileged document, from the office where it is maintained, except in the performance of official duties and authorized by law.

Any knowledge of a violation of this code must be reported immediately to the violator’s supervisor. Violations may lead to disciplinary action, including dismissal. Violations may also lead to criminal and civil liability.

Your signature below indicates that you have read, understand, and will comply with the above Code of Responsibility for Security and Confidentiality of Records and Files. This agreement shall be effective when signed below or in counterpart, photocopy, facsimile, electronic or other copies shall have the same effect for all purposes as an ink-signed original.

____________________________________________  _________________________
(Your signature)                          (Date)

IS Approval:

________________________________________  ______________
(Director/Associate Director of Systems & Operations)  (Date)

Training Verification:

________________________________________  ______________
(Exchange Administrator, IS Systems & Operations)  (Date)

Internal use only

IDM       RBAC