Request the Creation and Changes to Security Access Groups

1. Purpose

This Process Guide describes the process for requesting the creation and managing changes to ERMS security access groups. This is an activity undertaken by ERMS Powers Users and the ERMS Administrator.

2. Introduction

As an employee of the ANU you are required to retain records of the business activities you undertake on behalf of the University. The ANU policy on records and archives management states that staff will:

- document activities performed and decisions made on behalf of the University, and
- incorporate records created and received into the University's recordkeeping systems.

In order to comply with legislation and ANU policy it is essential that relevant records be held within ERMS.

3. Documents referred to in this Process Guide

ERMS Record, Location and Access (RLA) Spreadsheet

4. Abbreviations used in this Process Guide

**CRS:** CRS refers to the University's paper based records management system called Central Records System. CRS paper files are either digitised and available in ERMS, or not digitised but information about them (metadata) is available in ERMS.

**ERMS:** Is an acronym for Electronic Records Management System

**RLA:** ERMS Record, Location and Access (RLA) Spreadsheet

**ServiceNow:** Is the ANU Service Desk which provides IT support for all ANU staff and students. It allows ERMS enquiries to be logged and tracked.

5. Process Information

ERMS has been developed in order to promote transparency and sharing of information across the University.
Folders created within ERMS can be accessed by all ERMS users unless otherwise secured, i.e. security is applied as the exception rather than the rule. There may be instances where there is a requirement to secure folders which contain private, confidential or other sensitive information. These folders may need to be restricted to a particular work area or a group by establishing a security group that restricts access to the folders to staff belonging to that group. University Records staff are able to set up new security groups.

For staff files, you will only have access to staff files of your direct reports. Those who do not have access to these folders will not see or be able to search for a folder or the records within a folder.

Access to unclassified student files will be based on student administration roles within the student administration system. Further work is being undertaken to determine authorisation of staff access levels to classified student files on a need to know basis. If a supervisor who does not have access to the student folder requires information regarding a particular student they will have to request this through an authorised Student Administrator.

In some circumstances, because of their role in the University, staff may belong to a security access group which would allow access to their own file. Accessing your own file is inappropriate and does not meet the requirements of the ANU Code of Conduct. If you access your file, this is audited automatically by the system. A report is generated and sent via email to either the Director, HR or Student Administration for action.

The folder structure for all other records will have an open security model and records will be available to all users unless manually locked down by the ERMS Administrator or Power User.

Security access group creation and application occurs throughout the ERMS folder development process.

**ERMS Folder Development and Access Process**

<table>
<thead>
<tr>
<th>Steps</th>
<th>Responsible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>ERMS records folders and access identified</td>
</tr>
<tr>
<td>Step 2</td>
<td>Folders created in ERMS</td>
</tr>
<tr>
<td>Step 3</td>
<td>ERMS folder security access groups created</td>
</tr>
<tr>
<td>Step 4</td>
<td>Security access applied to folders</td>
</tr>
<tr>
<td>Step 5</td>
<td>Communicate ERMS folders ready for contribution</td>
</tr>
<tr>
<td>Step 6</td>
<td>Staff contribute records to ERMS folders</td>
</tr>
</tbody>
</table>

**REFERENCE GUIDES/TEMPLATES**

- Ref: ERMS Record Identification Checklist
- Ref: CRS Functional Folder Tipes List
- Ref: ERMS Naming Convention Guidelines
- Ref: ERMS Record Location, Access Spreadsheet
- Template: ERMS Record Location, Access Spreadsheet
- Ref: Business Classification Scheme
- Ref: ERMS Record Location, Access Spreadsheet
- Ref: CRIS Functional Folder Titles List
- Ref: ERMS Folder Creation and Tiling Conventions
- Template: Local Area ERMS Record Location and Access spreadsheet
- Template: Business Process ERMS Folder Structure and Access spreadsheet
- Template: Communication: Area Process ERMS Folder Structure and Contribution Groups
Security Access Group Creation Process Steps

1. Enter folder tiles in the ERMS Record, Location and Access Spreadsheet

2. Decide if the folder is open or restricted to a security access group

   In completing the ERMS Record, Location and Access Spreadsheet a decision is made whether the records are sensitive and require restricted access.

3. Name the security access group

   A number of approaches can be taken to naming access groups. The access to particular folders may be based on a role, in which case the role would serve as the access group name, e.g. Student Administrators. If a management level requires access to the folder then the security access group name would identify the location of the group and management level, e.g. Facilities and Services Senior Management Group.

4. Identify Security access group membership

   Once the name of the access group has been determined a list of the staff members and the University Identification (UID) Numbers are recorded against the Access Group name in the ERMS Record, Location and Access Spreadsheet.

   More than one security access group can be recorded as requiring access to an ERMS contribution folder.

   Once security access group members are individually recorded (names and UID) as part of an access group, from that point only the access group name needs to be used.

5. Obtain approval of the folders and access groups

   The final activity in the Business Process step is for approval to be obtained from the person authorised to approve the creation of the folder and the access group.

   The Power User sends the Record, Location and Access spreadsheet to the approver. In the case of university wide business processes folders, the Service Division Director must always be the folder and access approver.

   Once the Service Division folder structures have been approved, the service division folders, records and access are copied across to the Business Process ERMS Folder Structure and Access spreadsheet (Process Guide 6). This template is used as a formal advice of business process folder creation and record contribution conventions and communicated to all individuals involved in the business process e.g. Student Administrators. Approval is provided via an email confirming the folder structure and access groups.

6. Folders created in ERMS

   The Power User creates folders within ERMS referring to the ERMS Power User Reference Guide. Please note that prior to security access groups being applied to a folder, records within that folder are accessible by all ERMS users. No records should be included in the folder prior to applying the security access groups.

7. Power User sends Record, Location and Access Spreadsheet to ERMS Administrator for creation of security access groups

   The Power User sends the list of access groups and membership to ERMS Administrator via ServiceNow request. ServiceNow is the ANU Service Desk which provides IT support for all ANU staff and students. It allows ERMS enquiries to be logged and tracked.

8. ERMS Folder Security Access Groups Created

   The ERMS Administrator creates the requested security access groups and advises the Power User of creation and location of security access groups.
9. Security access applied to folders

Power User receives advice from ERMS Administrator via ServiceNow request reply that security groups have been created and are ready to be applied. The Power User applies the security access groups to the folders already created.

10. Communicate to staff that records can be contributed ERMS folders

Communication is issued to relevant staff of ERMS folder structure and contribution groups. This communication can be sent by the either the Power User or ERMS Business Process Folder structure approver, i.e. the Service Division Director or Local Area Management.

Staff members can refer to the ERMS User Reference Guide which provides a step by step explanation of how to contribute a record.

End of Process

Completing a ServiceNow Request

The ServiceNow request will go to the ERMS helpdesk managed by University Records and as required redirected to the ERMS Administrator.

Login to ServiceNow https://itservicedesk.anu.edu.au/

Click on Create New Call

Select - Affected contact field: add your name

Select - Service Provider Field – Select e.g. Service Divisions from list

Select - Urgency – Select 3 – Low – Limited issue

Select - Short Description - Enter ‘Request for creation or change to security access group’

Select - Additional Comments: Include any additional information – text or attach documents

Select - Save and Exit

The ERMS Administrator will provide you with the outcome of your request via ServiceNow which is sent via email to you.

End of Process
Changing Security Access Group Membership or Name Process Steps

Changing membership of a security access group requires the completion of the Business Process ERMS Folder Structure and Access spreadsheet (Process Guide 6) or the Record, Location and Access Spreadsheet for an area.

1. **Update membership of the access group in the ERMS Record, Location and Access Spreadsheet or Business Process ERMS Folder Structure Access Spreadsheet**

Change the membership of the access group by removing or adding a member name and UID.

2. **Create a ServiceNow Request**

Write that you would like to change membership of a particular ERMS security access group and provide the following details in the additional comments section of the ServiceNow request:

- Name of the ERMS security access group
- Name and UID of persons to be removed or included

Attach the updated ERMS Record, Location and Access Spreadsheet or Business Process ERMS Folder Structure Access Spreadsheet to the ServiceNow request.

3. **Receive notification that security membership changes executed**

You will receive an update email regarding your ServiceNow request advising that the security changes have been made.

End of Process