# AATAMS Database Security Policy

## Logins

1. Security will be managed on an individual basis, with each user having their own username and password.
2. The role of system administrator will have the highest level of access with the ability to add, edit and delete any data in the database.
3. There will be no more than two users with system administrator privileges (note some eMII staff will retain the equivalent of these privileges).

## Projects

1. Group security will be managed as a facet of projects.
2. A system administrator will create a project and assign a project Principal Investigator (PI).
3. A Projects PI can:
   1. Add other members to the project and assign edit or read only privileges to those members.
   2. Can create and edit installations, tags, deployments … associated with the project
   3. Can create receiver data associated with deployments, …
4. Members of a project with edit privileges can alter project data may be given
5. A user added to a project will be given one of the first three levels of access described in 3 below.
6. There will be two levels of security for project members
   1. Read Only  
      The user may view data related to a project, but cannot edit or delete the data.
   2. Edit Access  
      The user may view and edit the data related to a project, but can’t delete data.
7. Only a System Administrator may delete data from a project.
8. Only a project Principal Investigator and System Administrators will have access to add and remove project users and grant their privileges.

## Deployments

1. A project PI (or their delegate) will be able to create equipment deployments
2. Deployments that are considered vulnerable to vandalism or theft can be flagged such that location data is scrambled when presented to, or downloaded by, a member of the public including indirect access through other systems (eg. IMOS portal)
3. Even if a deployment has been flagged such that location data is scrambled, registered users of the AATAMS database will have access to un-scrambled, accurate location data.
4. Deployments that have been flagged such that location data is scrambled will be reviewed annually by the AATAMS Data Management Committee as to the appropriateness of the data being flagged and changes made (in consultation with the project PI) where the Committee determine the flag in not required.

## Detections

1. A project PI (or their delegate) can upload detections data for a project and flag detection data from individual deployments as AATAMS (detections recorded on AATAMS equipment) or non-AATAMS (detections recorded on equipment not owned by AATAMS).

## Embargos on Detections

1. A project PI (or their delegate) can place an embargo on detection data from individual deployments. Embargos must be dated and will be no more than 3 years from the date of setting the embargo.
2. An e-mail will be sent to the project PI 3 months before the expiry of a detection data embargo.
3. Embargos cannot be set on detection data downloaded from AATAMS equipment (however, non-AATAMS tag data related to individual AATAMS sourced detections may be embargoed).
4. Irrespective of any embargo on detections data, detection data for tags entered by a registered AATAMS database user will be visible to all users who are members of the project under which the tag is created.

## Tags

1. A project PI (or their delegate) can create tag data associated with specific tag ID’s.

## Embargos on Tags

1. A project PI (or their delegate) can place an embargo on tag data. Embargos must be dated and will be no more than 3 years from the date of setting the embargo.
2. An e-mail will be sent to the project PI 3 months before the expiry of a tag data embargo.

## Embargos on Species

1. If a particular species is considered endangered or vulnerable to interference through the use of publicly available AATAMS data, an embargo can be placed on detection data related to the particular species.
2. Embargos on species can only be set by a System Administrator. Users requiring a species embargo may contact a Systems Administrator and request the embargo.
3. All embargos on species are reviewed by the Data Management Committee annually.