IMOS ATF Data Security Policy

Logins

1. Only individuals from organisation, or individuals, registered to do animal research can access the database as a registered user.

2. Security will be managed on an individual basis, with each user having their own username and password.

3. 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.

4. Only a System Administrator can create, edit and delete the following data (items in parenthesis are database table names where it differs from the item):

    a. Organisation, Person, People in Organisations (Organisation_Person),

    b. Project, Project Role (Role),

    c. Device Type, Device Model, Device Manufacturer, Deployment Event Type, Mooring Type, Installation Configuration (Installation_Conf),

    d. Measurement Unit, Measurement Type, Treatment Type, Classification Level, Classification, Implant Type.

5. There will be no more than two users with system administrator privileges (note some eMII staff will retain the equivalent of these privileges).

Projects

6. Group security will be managed as a facet of projects.

7. A system administrator will create a project and assign a project Principal Investigator (PI).

8. A Projects PI can:

    a. Add other members to the project and assign edit or read only privileges to those members.

    b. Can create and edit the following data:

        i. People and their role in projects (Project_Role_Person), Editing right of project members (no current table),

        ii. Device, Device Deployer, Deployment Event, Installation, Installation Station, Receiver Deployment, Detection(s), Deployment Download, Download File, Download Tag Summary,

        iii. Surgery, Surgery Person, Animal, Measurement, Tag Release.

9. A user added to a project will be given one of the first three levels of access described in 10 below.

10. There will be two levels of security for project members

    a. Read Only
    The user may view data related to a project, but cannot edit or delete the data.

    b. Edit Access
    The user may view and edit the data related to a project, but can't delete data (This level of access to the project is the same as the PI's access to the project).

11. Only a System Administrator may delete data from a project.

12. Only a project Principal Investigator and System Administrators will have access to add and remove project users and grant their privileges.

Deployments

13. A project PI (or their delegate) will be able to create equipment deployments

14. 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)

15. 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.

16. 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

17. 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).

Tags

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

Embargos on Tags

19. A project PI (or their delegate) can place an embargo on tag data. Embargos must be dated and will be no more than 12 months from the date of setting the embargo.

20. An e-mail will be sent to the project PI 3 months before the expiry of a tag data embargo.

21. Initial embargoes can only be extended after review and recommendation by the AATAMS Scientific Committee or their delegate.

Data Visibility

22. With regard to data visibility, there are four types of user:

    a. Detection Data Owner (includes any member of a project allocated to the detection data)

    b. Tag Owner (includes any member of a project allocated to the tag data)

    c. Registered AATAMS User

    d. Public Access User

23. With regard to location data (either Installation Station location or location recorded as part of detection data), there are two types of visibility based on user type:

    a. Detection Data Owner, Tag Owner and Registered AATAMS User can still see accurate location data

    b. Public Access User can only see location data expressed in decimal degrees and truncated to two decimal places.

24. When a tag data embargo is in place:

    a. The tag Owner can see the tag data

    b. Detection Data Owner, Registered AATAMS User and Public Access User cannot see the tag data.